

CSO

THE RESOURCE FOR SECURITY EXECUTIVES

How to Win at Risk

STARTING ON PAGE 28

Reasons—and formulas—for calculating an ROI for security **PAGE 30**

Budget surveys exposed **PAGE 38**

Adding up the costs of a security breach **PAGE 40**

An economist's viewpoint: The art of uncertainty **PAGE 44**

Can cyberinsurance cover your assets? **PAGE 50**

Exostar Chief of Security Jeff Nigriny uses hard numbers to stand his ground on security projects.

Introducing **UnityOne™** from **TippingPoint Technologies**

The Active Network Defense System that Protects Networks at 2 Gbps

UnityOne™ is a security breakthrough. It is an ultra-high performance active network defense system that blocks network attacks before critical resources are damaged.

Full 2 Gbps Network Defense System

Software-based solutions running on Pentium®, SPARC™, or MIPS processors are too slow to offer real-time network defense. UnityOne is built on custom security-specific processors designed for ultra high-speed network security applications.

Stops Worms, Viruses, Trojans, Blended Threats, DDoS

Blocks thousands of attack-types based on absolute attack filters.

Digital Vaccine™ Update Service

Digital Vaccines™ are developed and delivered by TippingPoint's Threat Management Center which monitors over 10,000 sensors around the world to rapidly inoculate UnityOne systems against first-strike attacks.

High Availability Mode

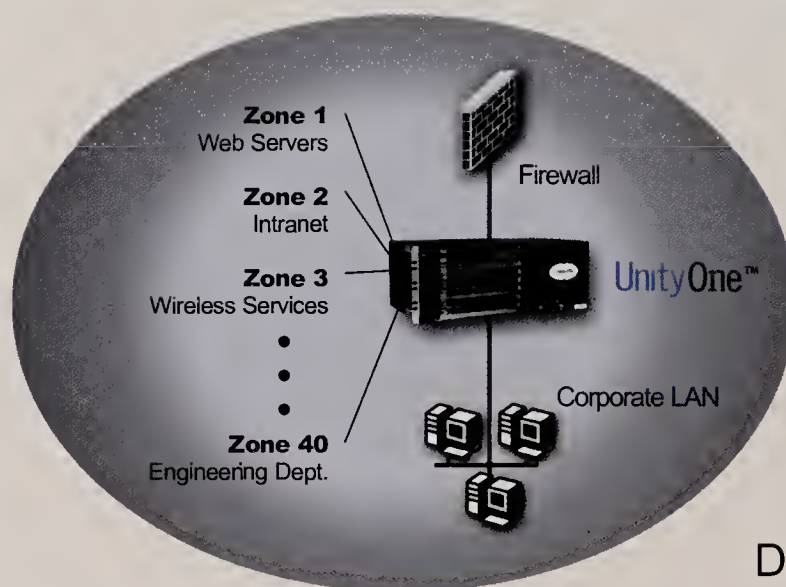
Active-Active Redundant Protection.

Up to 40 Physical Security Zones

Prevents both external and internal attacks. Security policies can be set to protect by user, department and site.

Protect.

Active Network Defense



Active Network Defense Architecture

UnityOne becomes a seamless element of the network infrastructure - shooting down Internet and Intranet attacks in real time. In delivering pre-emptive network defense, UnityOne is unyielding to hostile information attacks. Worms, viruses, trojan horses, blended threats, multi-headed threats, hybrid attacks, DoS and DDoS attacks are all vanquished at 2 gigabits per second.

A Level of Security Beyond the Firewall and IDS

Network defense systems are an emerging class of products that significantly improve network security.

UnityOne Defends at 2 Gbps

UnityOne performs high-speed packet and flow reassembly, stateful inspection, packet classification and unanchored content searching. The following table shows UnityOne's performance in terms of Intel® Pentium® Equivalents (PE).

Packet Size	UnityOne™ Pentium Equivalents*(PE)
64 bytes (Fragmented Attacks)	78 PE
384 bytes (Avg. Enterprise Packet Size)	42 PE
1500 bytes (Max IP Packet Size)	21 PE

*Intel® Pentium® III 1 GHz, 768 MB RAM when applied to Intrusion Blocking.
Performance metrics derived from NSS Group - Europe's foremost independent network and security testing organization.

UnityOne's processing capabilities include:

- TCP session flow reassembly
- IP and UDP fragment reassembly
- Session state tracking at 250,000 sessions per second
- Application layer protocol decoding
- Full regular expression matching across multiple packets

Fast.

at 2 Gigabits per second

Stop attacks. Now.

Why settle for simply detecting attacks... when you can stop them in their tracks. By deploying UnityOne, our customers realize a significant return on investment (ROI) by preventing network downtime and theft of their mission critical assets.

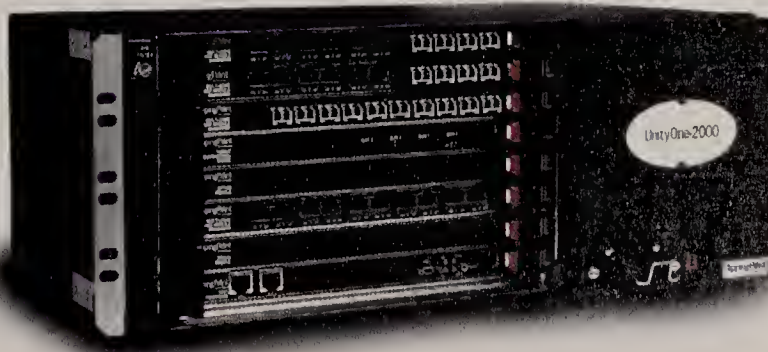
Call a TippingPoint Security Specialist today at **1-88UNITYONE** to find out how you can start blocking attacks and achieve your own immediate UnityOne ROI.

To learn more, visit us at www.tippingpoint.com to obtain your free *Active Network Defense Systems* white paper and also gain access to the new *SANS Critical Vulnerability Analysis Report*.

UnityOne strengthens the effectiveness of firewalls by blocking hostile traffic that has infiltrated open ports. And while IDS products are somewhat useful in cleaning up post-attack damage, the amount of information and number of alerts they generate can be overwhelming. But with UnityOne, blocked attacks cause no damage. Period.

UnityOne™

from **TippingPoint Technologies**



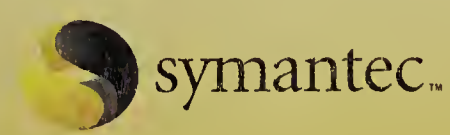




*Protection in every location.
Managed and integrated
from one location.*



Introducing the Symantec™ Security Management System. For the first time, security data from multiple locations, multiple tiers — even multiple brands of information security products — can be managed with a single system, at a single console. Which means that enterprise-wide policy compliance is finally a real possibility. It also means that because you've simplified your environment, you can reduce your operating costs. And, most importantly, you can now be more responsive to new and emerging threats, eliminating them before they do damage. It's part of a revolution in information security, a revolution that offers better protection, efficient management and ensured business continuity for your entire enterprise. For our latest White Paper, "Managing Security Incidents in the Enterprise," visit <http://ses.symantec.com/USA659A8VE> or call 800-745-6054.



contents

December 2002

VOL. 1, NO. 4

"If you stop and think about the real effect of security, in addition to perhaps mitigating risk, you've probably slowed things down."

-FRANK BERNHARD,
OMNI CONSULTING GROUP,
PAGE 44

SPECIAL
REPORT

How to Win at Risk

28 Risk: A Whole New Game

INTRODUCTION Economics is changing information security. You can help write the new rule book.

By Sarah D. Scalet

30 Calculated Risk

RETURN ON SECURITY INVESTMENT

Sure, determining an ROI for security is difficult. But it's also the key to selling your budget. Here's our three-step guide to getting started.

By Scott Berinato

38 Inside the Sausage Factory

BUDGET BENCHMARKS You wanted numbers. You got numbers. But ingest these budget surveys at your own peril. *By Derek Slater*

40 It's Not Easy Being Breached

THE COST OF A BREACH Surviving a security incident is just the beginning. Then you need to figure out what it really cost.

By Simone Kaplan

44 The Art of Uncertainty

INTERVIEW To hear Frank Bernhard tell it, economics is anything but the dismal science—and risk management is the key to a CSO's success.

50 Safety at a Premium

DECIPHERING CYBERINSURANCE Are your intangible assets protected? Here's how to choose the right insurance policy for your company.

By Daintry Duffy

COLUMNS

24 Securing the Network

SECURITY COUNSEL Larry Bickner, vice president and information security officer of Nasdaq, answers readers' questions.

26 Is the Sky Really Falling?

FLASHPOINT A CSO who spreads security paranoia is only making his own job harder. *By David H. Holtzman*

60 The Best Defense Is a Firing Offense

CSO UNDERCOVER What's a CSO to do when his tech expert says No to a request? *By Anonymous*

DEPARTMENTS

15 Briefing

A victory for the good guys; The Feds' most wanted; 2003 resolutions: Staking out new territory; Tag, you're it.

22 Wonk

In the eye of the holder: The government pushes biometrics to the forefront. *By Julie Hanson*

57 Machine Shop

Next year's hot security tools: Today's pain points are tomorrow's vendor opportunities. *By Simson Garfinkel*

64 Debriefing

Pop quiz: What are the odds?

Cover photo by
Drake Sorey;
illustration by
Jonathan
Barkat

IN EVERY ISSUE 6 CSOonline.com 8 Letter from the Editor 10 Letters 62 Index

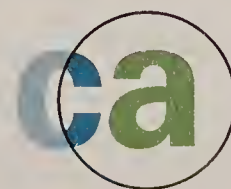


YOU'RE PROTECTED AGAINST HACKERS, VIRUSES AND WORMS.
BUT WHAT ABOUT ROSE IN BENEFITS?

eTrust™ Security Solutions

Complete protection for your entire enterprise.

When it comes to protecting your business, you need security that can protect your enterprise from potential threats, no matter where they may come from. That's exactly what eTrust does. Our family of products allows you to not only safeguard your entire enterprise, but also view and manage that security either centrally or from multiple delegated locations. So you can continue to grow and maximize new opportunities while minimizing your risk. And that's security you can feel secure about.



Computer Associates™

on the web at csoonline.com

Security Counsel

BUDGETS This month, Tina LaCroix, CISO of Aon, is available online to answer your questions about security budgets. Visit **SECURITY COUNSEL** to post a question. www.csoonline.com/counsel



Tina LaCroix

Free Newsletters

CSO newsletters delivered right to your inbox every month—for free. **CSO UPDATE** highlights the most recent content posted on CSOonline. **CSO WANTED UPDATE** alerts you to the latest security-related job openings in our database. It takes only a few seconds to subscribe.

www.csoonline.com/newsletters

News You Can Use

We scour the Web each weekday for the security headlines and stories you'll want to read, and we condense them so that you get up to speed fast. You can also dig deeper by clicking on a link to the full text of each article.

www.csoonline.com/news

Career Resources

Jump-start or advance your career with postings in our **JOB CENTER** and the listings in our **EVENT CALENDAR**. Need advice, ask our **CAREER ADVISER**, Joyce Brocaglia. Want to know who is where? Read **MOVERS & SHAKERS**.

www.csoonline.com/career

CSO Research Centers

Visit CSOonline's **RESEARCH CENTERS** for a wealth of information. Centers include archived articles from CSO and its sister publications, webcasts, interviews and links to relevant sources.

www.csoonline.com/research

Only Online

Check out the fresh content on CSOonline every weekday. Here's a rundown of what you'll find:

MONDAY

TALK BACK Should the feds cover up corporate hacks? Visit

each week to share your opinions on this and other controversial security topics.

www.csoonline.com/talkback

TUESDAY

SECURITY CHECK Quick and easy. Vote in our weekly security poll. You can also check the results of previous polls such as "Do you know how to calculate a return on your security investment?" Just 19 percent of respondents said they could.

www.csoonline.com/poll

WEDNESDAY

ANALYST REPORTS We've gathered research and analysis from respected sources and put it in one convenient package. Read about best practices for firewall deployments or worst practices in customer privacy management.

www.csoonline.com/analyst

THURSDAY

METRICS Did you know 40 percent of companies spend 5 percent or more of their IT budget on security? Visit each week for the surveys and statistics that businesses can count on. www.csoonline.com/metrics

FRIDAY

POLITICS & POLICY Read the full text of bills before the House and Senate, and blurbs about other legislative and political activity—inside the Beltway and out.

www.csoonline.com/politics



THE RESOURCE FOR SECURITY EXECUTIVES

President Walter Manninen

Group Publisher Gary J. Beach

Publisher Bob Bragdon

EDITORIAL

Editor in Chief Lew McCreary

Executive Editor Derek Slater

Managing Editor Elaine M. Cummings

Managing Editor, Production Cheryl R. Asselin

Senior Editor Daintry Duffy

Research Editor Lorraine Cosgrove Ware

Senior Writers Scott Berinato, Sarah D. Scalet

Staff Writer Simone Kaplan

Copy Chief Tom Wailgum

Asst. Managing Editor, Production Kathleen S. Carr

Copy Editors Kelli A. Gauthier (Assoc.),
Emily S. Henderson, Sarah Johnson (Assoc.)

Research Manager Lynne Z. Rigolini

Editorial Resource Manager Carol Zarrow

Editorial Assistants Daniel J. Horgan, Joe Sullivan

Contributors Larry Bickner, Simson Garfinkel,
David H. Holtzman, Paul Roberts, Martyn Williams

Editorial Operations Specialist Julie Hanson

DESIGN

Executive Director, Art and Design Mary Lester

Art Director Steve Traynor

Senior Designer Chandra Tallman

Design Group Assistant Rachel Barnett

WEBSITE

Senior VP/General Manager, Online Tim Horgan

Web Editorial Director Art Jahnke

Executive Web Editor Martha Heller

Web Editor Sandy Kendall

Web Writer Jon Surmacz

Online Technology Director Dagmar Eiben

Senior Web Developer Ellen Morey

Online Research Manager Kathleen Kotwica

Audience Development Manager Andrew Burrell

Web Developers Diane Chen, Shannon Macdonald

Online Content Researcher Tara Gillet-Liloia

Designer Graham White



C X O M E D I A I N C .

Founder Joseph L. Levy

INTERNATIONAL DATA GROUP

Board Chairman Patrick J. McGovern

CEO Pat Kenealy

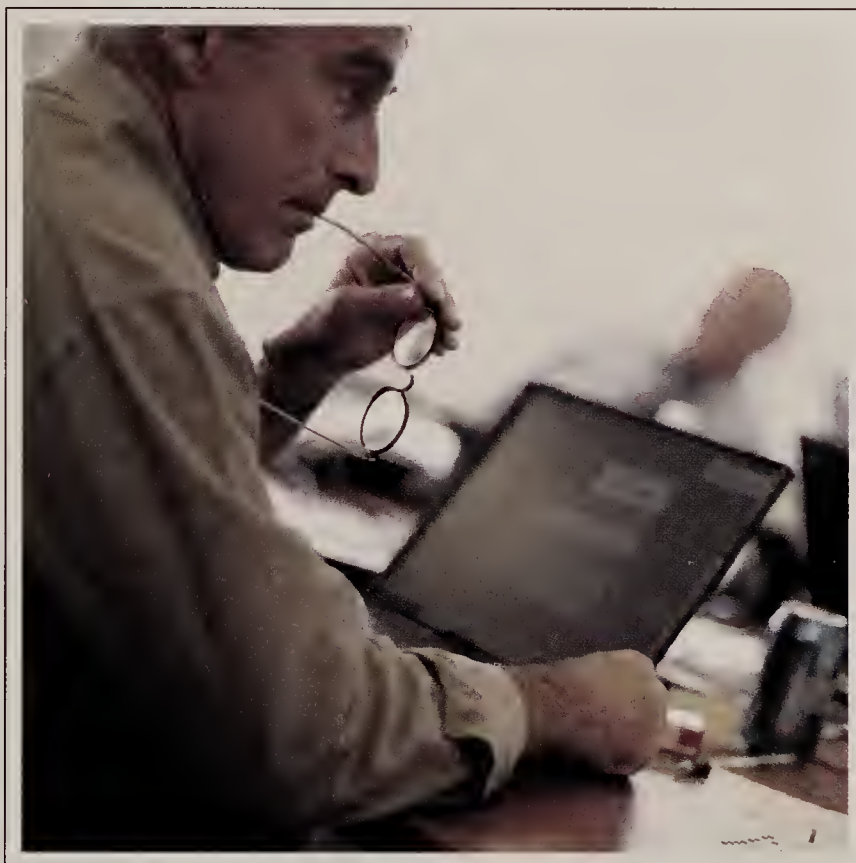
BPA INTERNATIONAL MEMBERSHIP

Applied for August 2002

© CXO Media Inc.

No. 1

BEARINGPOINT ON BUSINESS EMPOWERED.



In today's business world, you deserve more than just consulting. You need your business to be empowered with the right information. You also need a business partner that will help you to align your business and systems to your desired goals. At BearingPoint—

formerly KPMG Consulting—it's our culture to deliver the right solutions for our clients' businesses. It's the same way we have operated for over 100 years. By providing

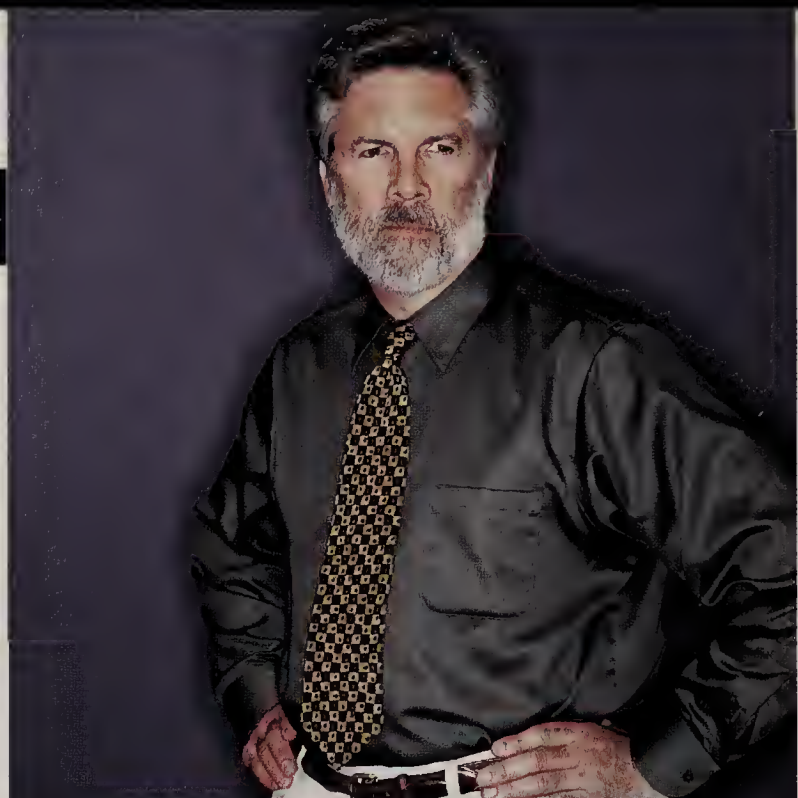
all of our clients access to the right knowledge and information that empowers their employees to effectively run their business systems. Because the right information brings knowledge. And knowledge is power. Sharing it is empowerment.


BearingPoint[™]

Formerly KPMG Consulting

Business and Systems Aligned. Business Empowered.[™]

STRATEGY & BUSINESS PROCESS | CUSTOMER RELATIONSHIP MANAGEMENT | SUPPLY CHAIN MANAGEMENT | ENTERPRISE SOLUTIONS
INTEGRATION SERVICES | INFRASTRUCTURE SOLUTIONS | EMERGING TECHNOLOGIES | MANAGED SERVICES



Ignorance Is Dis

Ignorance isn't always a bad thing. In fact, journalism makes a virtue—and a profession—out of ignorance. Good journalists are good at knowing what they don't know, and

even better at finding the people who *do* know. The best of the breed live to learn new things, to which end they doggedly seek out the smartest sources to fill in the blanks. The practice of the craft over the course of a career amounts mainly to identifying fresh pockets of ignorance to conquer. And, hey, it's a living.

Having launched this magazine in September, we've already traveled what feels like a very great distance from relative darkness to greater light. I will confess that, in the spring of 2002, when I faced the prospect of starting a publication about security (I had plenty of help, but I've learned that when confessing, it's always best to speak for yourself), I might have thought something along the lines of "Geez, what a snooze." That was the initial reflex of someone who hasn't yet learned what he doesn't know. Like security vulnerabilities, ignorance is blameworthy only when it remains unremediated. In fact, it wasn't long until, having started to scratch beneath the surface of the topic, I began to grasp the size and complexity of what's involved. Not simply a matter of firewalls and viruses and hackers, security began to resonate with issues political, ethical, behavioral, managerial, philosophical, physical, logical, technological, sociological, cultural, criminal and military. You name it, it's in there somewhere. And, so, I quickly learned: not such a snooze, after all.

Now we are rapidly discovering that the CSO role, practiced at the highest level, has its arms around just about every activity an enterprise undertakes. The CSO editorial staff met recently with members of the International Security Management Association (ISMA). As articulated by its current president, George Campbell (see Letters, November 2002), ISMA's position is that security is a broad unified activity, making no meaningful distinction between the physical and logical domains. The CSO's beat encompasses all categories of risk—from safeguarding executives in Bogotá to headquarters buildings in

New York to customer information in distributed databases.

Among the most intriguing broad subtopics within the security domain are the assorted economic arrangements that surround risk management. Of all the duties of the CSO, risk management—writ large, as in the ISMA rendition—is arguably the most important. Dan Geer, the CTO of a security consultancy called @Stake, notes that when security measures begin to consume too much productivity, they become "dis-economic." The role of the CSO is to make sure a balance is maintained between the solutions applied and their impact not just on vulnerability but on productivity and profitability as well. That is why we've dedicated our first special issue to helping readers prevail over risk. (The issue was spearheaded by Managing Editor Elaine Cummings and Senior Writer Sarah Scalet.) Risk management begins with an understanding of the business costs of unremediated vulnerability. Only when the costs are known can they be weighed against the economic potential of various business opportunities. Then the appetite for risk, in various quarters of the enterprise, can be expressed with reasonable accuracy.

While the focus of our examination of risk is corporate networks (where so much uncertainty still persists as to the costs of insecurity), the broader topic of risk management is relevant to all of the CSO's duties. We look forward to your reactions: mccreary@cxo.com.

—Lew McCreary

© 2002 PricewaterhouseCoopers LLP. PricewaterhouseCoopers is a firm of PricewaterhouseCoopers LLP and other members of the worldwide PricewaterhouseCoopers organization.

IT'S NOT OFTEN
BUSINESS GETS A
LESSON IN EFFICIENCY
FROM GOVERNMENT.
GET OUT YOUR NOTEPAD.

PRICEWATERHOUSECOOPERS 

Without dismantling any system or disrupting any department, we delivered security, access management and ROI to one state government. Skeptical? So was the state government until they launched our Identity Management solution. Want to discover the kind of ROI your organization can receive? Schedule a free assessment with our proprietary Identity Management Value Calculator ToolSM and learn how you can save time, money and resources. Call (800) 639-7576 or visit www.pwcglobal.com/roi. Write it down.

letters

csoletters@cxo.com



The Software Sound Off

I'M A FEDERAL PROSECUTOR WHO prosecutes high-tech crime, and I am in the process of editing and writing portions of a computer crime and information security book. Your article ["The Big Fix," October 2002] really nailed the software vulnerability issue. Indeed, it was the best one I have read so far. Keep them coming.

ELLIOT TURRINI
*Federal Prosecutor
Department of Justice*

I READ YOUR ARTICLE WITH GREAT interest. I have been looking at this problem and feel that there is a more systemic issue. The causes of insecure software are related to the causes of software failure. While a buffer overflow may enable a hack that provides unauthorized use, at its root it is a software bug that would cause software failure regardless. While I concur that the current generation of software developers has not been educated with respect to security, I think the bigger cause of sloppy coding is poor design.

For more than 30 years, marketing of computer systems has been evolutionary. The reasons for this are well documented and relate to IBM's loss of market share when its 360 system was introduced. There have been three major breaks in the evolutionary model: the rise of the PC as a replacement to the mainframe, the

replacement of PC operating software with a more functional base (Windows NT and Windows 95), and the rapid adoption of Internet technologies based on HTTP. However, none of those discontinuities has really been founded on comprehensive new architecture; the environment has evolved to embrace the previous systems and even provide backward compatibility. Part of the reason for a legacy problem is the baggage that we carry in the name of protecting a past investment.

ROGER COATES
*President
Masaccio Technology
rogercoates@earthlink.net*

"THE BIG FIX" IS DEAD-ON AND reflects exactly what the industry (and my company) is experiencing. Great article!

ROGER L. YEE
*CEO
ShadowLogic
ryee@shadowlogic.com*

THANKS FOR WRITING AN EXCELLENT article about poor quality software. However, the following quote from Oracle CSO

We want to hear from you.

To respond to articles you've read in CSO, write to us at csoletters@cxo.com. We welcome your criticism, thoughts and suggestions.

CSO

How to Reach Us

E-MAIL

csoletters@cxo.com

PHONE

508 872-0080

FAX

508 879-7784

ADDRESS

CSO Magazine
492 Old Connecticut Path, P.O. Box 9208
Framingham, MA 01701-9208

SUBSCRIBER SERVICES

phone: 866 354-1125

fax: 847 564-9453

e-mail: cso@omeda.com

REPRINTS

Reprints are available by calling Reprint Services at 651 582-3834, or via e-mail at csoreprints@reprints-services.com.

ABOUT IDG International Data Group (IDG), the leading global provider of IT media, research, conferences and events, informs more people about technology than any other company in the world. Offering the widest range of media options, IDG reaches more than 120 million technology buyers in 85 countries representing 95 percent of worldwide IT spending. IDG publishes more than 300 newspapers and magazines in 85 countries, led by the *Computerworld*, *Infoworld*, *Macworld*, *Network World*, *PC World* and *CIO* global product lines. IDG offers online users the largest network of technology-specific sites around the world through IDG.net (www.idg.net), a gateway to IDG's 330 websites powered by more than 2,000 journalists reporting from every continent in the world. IDG also produces 168 technology-related conferences and events, and research company IDC provides global market intelligence, analysis and forecasts in 43 countries.

Mary Ann Davidson bothered me because it typifies Teflon management. "If customers don't make security a basic criteria, they lose their right to complain in a lot of ways when things go bad." By analogy, the basic criteria of an automobile is that it serves as a reliable means of transportation. However, we expect the air conditioning, air bags, seat belts and windshield wipers to work for comfort and safety.

Using your analogy, buildings basically provide shelter, but we also expect the elevators, HVAC and other essential attributes to work for comfort and safety.

"Lose their right"—you've got be kidding!

DANIEL J. TISAK
Director, Bala Consulting Engineers

IN BIG TROUBLE

You're the king. Strong. Safe. Protected. Right? Wrong.

The fact is, if your network isn't protected by NetScreen, you could be far from safe. You see, technological advances don't only occur in the corporate world. Predators — inside and outside your network — have also made leaps and bounds. Trojan Horses. Worms. Nimda. Code Red. Denial of Service attacks. All emerging threats that many legacy security solutions just can't handle.

NetScreen can. NetScreen's line of purpose-built security systems and appliances has the flexibility and performance to handle new threats. And evolve with them. Keeping not only the central site connected and secure, but also your wireless LANs and remote offices. NetScreen's solutions offer integrated VPN, firewall and network attack blocking. All of which are key to keeping predators under control. And your entire enterprise out of trouble. Find out more about securing your place at the top. Download a white paper on protecting your network from the new generation of security threats at www.netscreen.com/ad/na_cs.





© 2002 All rights reserved. All trademarks, service marks, and registered trademarks of the United States Patent and Trademark Office are used herein. All other trademarks, service marks, and registered trademarks are the property of their respective owners.

Make every step count for more.



Nokia security appliances simplify network security.

Pre-installed, pre-configured and ready to go.

Whether they're being used for VPNs, firewalls, intrusion protection, or Internet traffic management, Nokia appliances are delivered ready for implementation. They're compatible with any IP network. Often, the only on-site requirements are powering up the appliance, connecting it to the network, and entering the correct IP address.

Nokia security appliances are designed for full remote management.

Easy-to-use GUI-based interfaces offer a full overview of security deployment, or a drill-down to the details, anytime. Deep collaboration with partners like Check Point Software Technologies, Internet Security Systems and F5 helps coordinate all the capabilities of their applications. So our customers can respond to internal and external threats, by upgrading or redeploying their equipment, quickly and more easily than ever before.

First Call-Final Resolution support eliminates the usual finger-pointing.

It's another way that our ongoing partnerships give our customers greater peace of mind. To download case studies, details and more, just visit www.nokia.com/ipsecurity/na.

NOKIA
CONNECTING PEOPLE

**In the Midst of the Telecom Storm...
SAVVIS Customers Know the Way.**



1-800-SAVVIS-1

www.savvis.net/testimonials

With all the turmoil in the telecom industry today, it's easy to feel like you've been caught in the "perfect storm." You worry that choosing the wrong network provider could leave your company vulnerable. Conversely, you worry that delaying decision-making could leave you behind the curve.

SAVVIS customers tell us they're on course. Their IP VPN is getting the job done for voice over IP (VoIP), global video conferencing, ERP, and more.

From Wall Street to Main Street, SAVVIS is the financially sound choice for people who demand a proactive managed IP service provider. SAVVIS has been delivering high performance IP VPN and managed hosting services to financial institutions, professional services firms, and retail enterprises for years. And, SAVVIS has one of the strongest balance sheets in the industry.

Don't just take our word for it. Visit our web site and discover what the Chicago Board Options Exchange, Looksmart, the Philadelphia Stock Exchange, RM Crowe, Shearman & Sterling, Fitch Ratings, Telezoo and so many others have to say about working with SAVVIS.

**Trust the Network that Powers Wall Street
to Empower your Business.™**

briefing

News, Stats and Fast Facts

Edited by Kathleen Carr
and Daintry Duffy

Bruce Schneier, Counterpane CTO, says that the recent DNS attack is a victory for the developers of security architecture.

tion. It's only when these cached copies expire—each one has a preset time to live—that real problems will start. Experts say that would take eight or nine hours.

"First and foremost, this is a success story," says Bruce Schneier, founder and CTO of Counterpane Internet Security. "The attack failed. The

architecture worked." In effect, we won!

Even so, the attack generated a buzz in both security circles and the mainstream media. Some posited that this was a practice run by terrorists. Others suggested it represented a new level of sophistication among hackers.

Not so on either count, others say. It was, after all, a relatively elementary type of attack easily dealt with. And many, including Schneier, laugh at the idea that this was a precursor to terrorist activities. "We know what the motive was," he says. "There can only be one: vandalism."

While Henny Penny is wrong—the sky is not falling—the attack should generate discussion. For example, right now the 13 root DNS servers are managed in a collegial, volunteer manner. Does this need to change? Should there be more root DNS servers, and if so, where? Are there ways to fortify the defenses of DNS and other architectures and protocols? (Border Gateway Protocol routing, or BGP, is another that's widely known to be vulnerable.)

Anyway, it's good to be able to apply 20/20 hindsight after a failed attack instead of a successful one. Chalk one up for the good guys.

—Scott Berinato

National Database Controversy in Japan

PRIVACY Local governments across Japan began inputting data into a new nationwide central database on Aug. 5, despite complaints from several quarters. Some complaints, such as those from privacy advocates, were expected, but things really began to heat up when several local governments said they wouldn't participate in the system until promised privacy laws were enacted.

The new system assigns everyone in Japan an 11-digit identification number, which he will use to access local government services. It replaces a system based on hanko—or small personal stamps. When it was proposed in 1999, the government attempted to silence critics by promising a new data-privacy law to be enacted before the database went into operation. But that law got bogged down with additions and the system went online as planned, leaving some local authorities to lodge complaints. Two cities in Tokyo—Suginami and Kokubunji—refused to connect, and Japan's second largest city, Yokohama, said it would enter citizens into the database only if they gave permission.

To date, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT), which is responsible for the system, hasn't divulged any technical information. In fact the MPHPT has refused to divulge the location of the database center, although it admitted it is somewhere in central Tokyo.

The privacy law is tied up in parliament, leaving the system in operation without legal protection against unauthorized use.

—Martyn Williams, Tokyo correspondent
for the IDG News Service

The DNS Attack: A Success Story for the Good Guys

INTERNET ATTACKS Just before Halloween this year, someone tried to take down the Internet by attacking the 13 root DNS servers, the computers that translate names like *www.blahblah.com* into their true numerical addresses. The attack failed, or, put another way, the architecture of DNS succeeded in staving off the attack.

The attacker used a brusque kind of distributed-denial-of-service attack called an ICMP flood that drowned the servers with 10 times the amount of traffic they normally handle. Only seven of the 13 servers were severely affected. At the height of the two-hour attack, packet loss reached 10 percent (it's normally less than 1 percent). At worst you got sluggish Web performance. Probably you didn't even notice.

That's because of how DNS works. Instead of just leaving these word-to-number translations on the root server, copies of them are cached all over the Internet on routers. That way you're not banging on the door of a DNS server every time you type in *www.blahblah.com*.

It also means when these root DNS servers are down most of us can still navigate by accessing a cached copy of the DNS informa-

Do you know how to calculate a return on your security investment?



For the 81 percent of you who confessed that you don't know how to calculate a return on your security investment, see "Calculated Risk," on Page 30. To participate in CSO Security Check polls, visit www.csoonline.com.

The Fed's Most Wanted

SOFTWARE QUALITY On Oct. 2, the General Services Administration released a list from The SANS Institute and FBI of the top 20 Internet security vulnerabilities to the public at a gathering of government CIOs and IT professionals in Washington, D.C. As in the past, this year's SANS/FBI top 20 list sounded warnings about Microsoft's Internet Information Server (IIS) and Internet Explorer Web browser.

For users of the Unix or Linux operating systems, vulnerabilities in the Apache Web server were listed as well as holes in commonly used tools and protocols such as SSH (secure shell), SNMP (simple network management protocol) and FTP (file transfer protocol).

The government is pushing free and premium services offered by vulnerability scanning companies to help organizations identify the vulnerabilities on their networks.

"You can't implement a program like this without tools," says Alan Paller, research director at The SANS Institute. "How do you find the machines with the problems? You would have to manually scan every machine."

In prior years, Paller says, SANS offered only the list or offered free detection tools that were not commonly used.

"The breakthrough this year is that you can use the tools you already have," says Paller, who notes that 90 percent of the scanning market is covered by Internet Security Systems and the Nessus Organization.

While the hand-in-glove nature of the scanning industry's relationship to the SANS/FBI top 20 list might cause some to wonder whether the list is serving the public as much as the bottom line of the major security vendors, Paller says that the cooperation of such companies is absolutely vital in the job of assembling an accurate list for companies to use.

—Paul Roberts

The Pitfalls of VoIP

COMMUNICATIONS Voice over IP (VoIP) is a fast-emerging communications technology that allows organizations to send voice traffic over IP networks. Many businesses, however, are concerned about the reliability and security of VoIP technology.

For those who embrace it, VoIP offers its users local and long-distance phone service at a fraction of the cost of analog voice communications. In addition, VoIP promises to deliver a whole world of new features to the workplace that tie together voice and data. Forget about caller ID—imagine a phone that ties the incoming caller ID directly to your customer database, automatically pulling up customer accounts on your support representative's desktop.

But CIOs and CSOs tread carefully when considering alternatives to the existing phone infrastructure. While getting an e-mail bounced back to them might make customers wonder whether you're having server troubles, getting a phone call to your headquarters dropped might make them wonder whether you've gone out of business.

According to Matthew Kovar, director of security solutions and services at the Yankee Group, the first thing CSOs should understand about VoIP security is that they already know a lot about it.

"Voice is just a different application that's going to run over IP infrastructure, so all the vulnerabilities that exist in your other IP applications also exist in this application," says Kovar.

Among the key exposures of VoIP systems, he says, are traditional hacks such as snooping (intercepting and decoding VoIP traffic) and packet spoofing (impersonating a party in a VoIP exchange to collect data).

The challenges of VoIP have made virtual private network (VPN) technology the choice for most CSOs.

Using VPN, companies can encrypt wide-area VoIP traffic from remote offices and send it over VPN tunnels, keeping that voice content secure. Using VPN also eliminates the need to open ports on the corporate firewall to allow VoIP traffic through.

Still, the landscape is changing with hardware manufacturers like Cisco Systems and Check Point Software Technologies adding SIP and H.323 support for their existing firewall products.

In addition, smaller players like the Swedish company Ingate are marketing firewalls designed specifically for VoIP traffic.

In the end, CIOs and CSOs will have to become convinced that reliable answers exist for the security questions posed by VoIP before the technology will take off.

"It's a question of whether customers feel comfortable with IP issues that may interrupt phone networks, and right now they just don't have enough experience with the technology," says Kovar.

—P.R.



Rock Solid Security

Jonathan Franklin
Trial lawyer

Jonathan Franklin, P.A., a boutique law firm based in Miami, Florida, represents corporate clients around the country. The firm specializes in product liability and tort law.

"There were several factors that went into our decision to choose CyberGuard. Chief among these was its proven secure track record. Independent data, reports and evaluations also revealed the product's overall excellence. And we were particularly gripped by its hardened OS, powerful VPN and obvious rock solid security.

"The Internet, with its continuous connections, acts as a doorway directly into your office. It offers a way out to the world and, more importantly, a way in for the world. At our firm, we maintain and store confidential and privileged materials, as well as trade secret information. As a result, we could not risk choosing a product with any vulnerability when we undertook steps to secure our office and valuable information. Frankly, knowledge of any vulnerability alone is enough to stick you with legal liability.

"Faced with the prospect of having to spend \$10,000 to \$12,000 to get the quality and performance in this caliber of a product, you also need to weigh the potential legal liability. In our opinion, one breach could expose any company to millions in liability. And that was not a risk we wanted to take."

CyberGuard's security solutions are found in Global 2000 companies and governments worldwide. CyberGuard's award-winning, premium firewall/VPN appliances maintain complete separation of network traffic from system components.



Firewall/VPN Appliances

For white papers on Rock Solid Security go to:
www.cyberguard.com/ROCKSOLID/home.cfm
Phone: 954.958.3878 • e-mail: info@cyberguard.com

Copyright 2002 CyberGuard Corporation. All rights reserved.

CYBERGUARD®
WORLDWIDE
DEFEND YOUR DOMAIN

2003 Resolutions: Staking Out New Territory



Bruce H. Bonsall | CISO | MassMutual Financial Group

- I resolve to further instill in my organization the need to plan for security rather than consider it at the last minute. We've gotten much better at that in recent years but still have a little way to go.
- to treat security even more as the business process that it is and less as a series of technical implementations.
- to spend more time on planned activity and less on reacting to crises, or should I say, perceived crises.



Matthew Speare | Director of IT Risk Management | Ohio Savings Bank

- I resolve to update my privacy policies.
- to conduct comprehensive distributed systems disaster recovery tests.
- to find a practical use for public-key infrastructure.
- to find a way to encrypt all customer information.
- to increase the security awareness in my organization.
- to stop "power users" from being able to download and install shareware from the Internet.



Rick Ramsey | Director of IT Risk Management | Bank One Investment Management Group

- I resolve to improve security awareness throughout the organization.
- to centralize distributed security administration functions.
- to implement a shared authentication environment leveraging single sign-on capabilities.
- then, we can go after world hunger....



Micki Krause | CISO | Pacific Life Insurance

- I resolve to provide security education and training. Building an effective security awareness campaign doesn't incur enormous expense, but the resultant increase in awareness significantly impacts the mitigation of risk. Security education, done correctly, makes everyone in the company a deputized part of the program.



James R. Wade | Senior VP and CISO | KeyCorp

- I resolve to improve response time for information security service requests.
- to continue to increase security awareness across the organization.



John A. McCarthy | Executive Director of the Critical Infrastructure Protection Project, National Center for Technology & Law | George Mason University School of Law

- I resolve to expand the role of cooperative cybersecurity arrangements such as those begun by The SANS Institute concerning industry standards setting for cybersecurity.
- to work to break down the barriers that exist for true information sharing among the critical infrastructure sectors (government, industry and academia).



Chris Price | Director of Corporate Security Svcs. | Hydro One Networks

- I resolve to continue to promote the most cost-effective and visionary approach to asset protection being the "security triangle" (people security, information security and physical security).
- to try to determine new and improved methods to measure and quantify the value of security in an attempt to avoid an event epitaph of "security is always excessive until there's not enough."

"I'm not saying there's not a federal role. I'm saying the opposite. There is a big federal role. But it's not regulation."

—RICHARD CLARKE, SPECIAL ADVISER TO THE PRESIDENT FOR CYBERSPACE SECURITY, DURING A VISIT TO *CSO* MAGAZINE, ON THE DRAFT CYBERSECURITY STRATEGY

Before you can prioritize security gaps, you have to see them

>	Systems Integration.
>	Outsourcing.
>	Infrastructure.
>	Server Technology.
>	Consulting.

first.

We built a unique planning process that will help you identify security gaps across your organization. It's a powerful, comprehensive approach to help you evaluate risk and set priorities.

Unisys Zero-Gap Security PlanningSM discerns security gaps throughout your organization, assessing physical, operational, cyber and financial risks.

It's the holistic viewpoint that brings security to a business integration level, giving you the flexibility to prioritize immediate needs, focus resources and change processes. Unisys supports your planning with superior services for Business Continuity. IT Infrastructure Protection. Privacy. Collaboration. Identity.

Zero-Gap Security Planning. With precision thinking, relentless execution to drive your vision forward. Thinking focused on where you need to prioritize security. Execution focused on efficiency, affordability and totally practical results.

So, that vision you have... to know every security gap, to prioritize risk... Imagine it. Done.

UNISYS

Imagine it. Done.

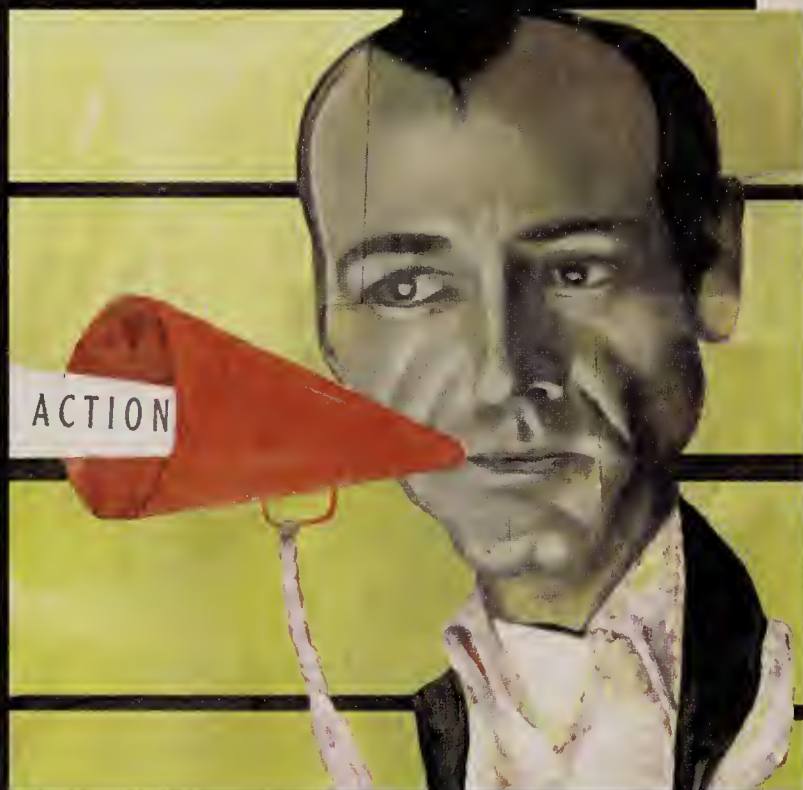
For more information on Zero-Gap Security Planning, call 800.874.8647 ext 792 or visit www.unisys.com/security

Briefing

An Unusual Suspect

CORPORATE TRAINING "I'm ready for my close-up, Mr. Spacey!"

He freaked you out as a gruesomely creative serial killer in *Seven*, intrigued you with tales of Keyser Soze in *The Usual Suspects* and drew you into his fatal crush on a teenage cheerleader in *American Beauty*...but what does Kevin Spacey have to do with corporate security? Quite a bit, it turns out. Spacey's film company Trigger Street Productions is partnering with former hacker Kevin Mitnick and his new consulting company Defensive Thinking to produce a series of security awareness training films to help companies protect against Mitnick-style social engineering exploits.



The films will address broad IT security issues like viruses but are also likely to cover best practices around personal security issues like identity theft. According to Mitnick, the films will be 45 minutes in length and are due out in the spring of 2003. Far from the usual amateurish corporate video fare, Mitnick will be narrating the films, and the cast will be made up of professional actors and actresses. So, CSOs can finally entertain themselves with wondering who'll be playing them when the day-to-day struggles of managing corporate security finally make it to the big—or in most cases small—screen on wheels.

—Daintry Duffy



Um, I forgot my card.

the CSO, that translates into at-the-door programmability. CSOs can reprogram a user's access card, changing encrypted information on the fly as employees enter the door.

ACCESS CONTROL Radio frequency identification, or RFID—a data collection technology that uses electronic tags to store data—sounds like IT fiction, but at Texas Instruments, eMarketing Manager Bill Allen and the RFID systems team have been using it to track livestock for years.

Texas Instruments has since migrated (pun intended) to using RFID for access control. "Corporate security managers are seeking a higher level of security, driven by the events of last September," says Allen. Texas Instruments manufactures the readers and the cards for access control systems using 13.56MHz technology, which allows for 2Kb of data storage. For

Corporate security managers were looking to combine radio frequency identification with biometrics, but previous RFID cards couldn't hold enough data for biometric tagging. Since the cards can now hold 2Kb, biometrics is possible in addition to increased levels of encryption.

And what would security be without convenience? These multifunction cards can act as time cards, control an employee's access to the building, serve as the currency with which they purchase lunch and even provide access to the office parking lot, which is more than the cows ever had.

—Kathleen S. Carr

MIND YOUR PHYSICAL SECURITY

70%

of senior IT managers are reviewing physical access to corporate premises and computers, along with monitoring and identifying IT security vulnerabilities.

SOURCE: DEFCOM INFORMATION SECURITY

BUSINESS TRIVIA QUESTION

Number 19

VeriSign processes over
\$3.7 billion in payment transactions
per quarter.

☐ True?

or

☐ True?

It may also be news to you that VeriSign handles e-commerce payments for some 80,000 different businesses and protects more than 400,000 websites. You see, VeriSign has spent the last seven years building a secure infrastructure for the Internet. We'd like to do the same for your business. VeriSign can help you deploy a trusted infrastructure so you can conduct secure communications and transactions. So no matter how many e-commerce payments your company handles, you'll know every last one of them is secure.

*Learn all you need to know about infrastructure security – and how VeriSign's managed network and security solutions can help you – by downloading our new white paper: **Cyber Security in the Age of Action**. Visit www.verisign.com/security*



■ PAYMENT SERVICES ■ TELECOMMUNICATION SERVICES ■
■ NETWORK AND SECURITY SERVICES ■ WEB IDENTITY SERVICES ■

© 2002 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.



In the Eye of the Holder

The government pushes biometrics to the forefront By Julie Hanson

AMES BOND IS NOT the only one who depends on the wizardry of biometric tools like retinal scanning and voiceprint analysis. Agencies in charge of border and transportation security, as well as the military, are facing mandates requiring them to use biometrics.

The Defense and State departments are already using biometric smart cards for building access, and the FAA is required to examine biometric identification for its employees under the Aviation Security Act, passed in 2001. The Driver's License Modernization Act, which calls for biometric licenses, is the closest the general public has come to the possibility of mandated biometrics. But the act hasn't seen any movement since May, the same month it was introduced to the House of Representatives, and a January proposal from the American Association of Motor Vehicle Administrators calling for nationwide biometric licenses has gained little acceptance.

Before government officials move forward on any biometric usage, they need accuracy standards, so they've enlisted the National Institute of Standards and Technology (NIST) for help. A team of 15 is focused on determining the accuracy of current fingerprinting and face-recognition biometrics. Congress is scheduled to review the NIST's initial reports. They'll be available on NIST's website, www.nist.gov.

Martin Herman, NIST's information action division chief, says his department's current biometrics' standards research is driven mostly by two bills with steadfast deadlines: the USA Patriot Act, signed by the president in October 2001, and the Enhanced Border Security and

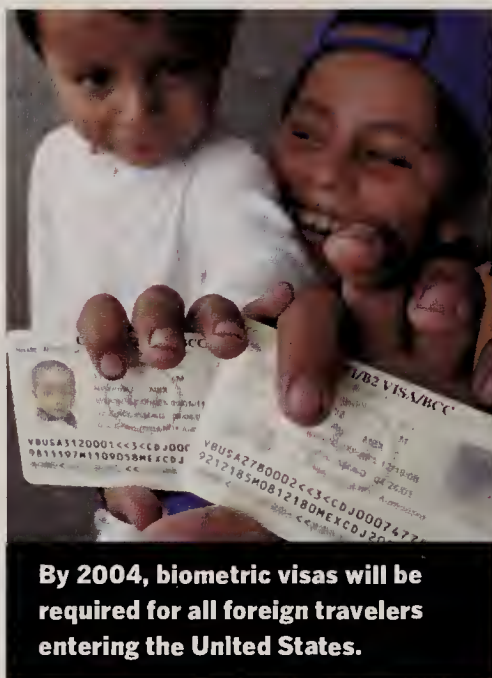
Visa Entry Reform Act, passed this May. Both bills mandate increased border security and the use of biometrics by as early as 2004, when foreign travelers will need biometric visas to get into the country.

To meet those deadlines, officials will have to deal with the many variables of biometrics. Using recognition software to identify a face in a dim hallway is harder than if that person were in a well-lit room. And human error comes into play with fingerprinting. "We are running tests across these large databases and getting accuracy numbers of systems and algorithms," Herman says. "We use hundreds of thousands of samples from the State Department obtained in actual exam-

ples of people using travel documents."

For the next couple of years, the federal government will be the number-one consumer of biometric technologies, according to Paul Collier, executive director of The Biometric Foundation. Collier calls the government "the perfect candidate" with its numerous facilities and staff strewn across the country. And, you could assume, the power to mandate that its own employees use the technology.

While the government might concur, average citizens are likely to be another matter entirely. When it comes to surrendering a thumbprint to the government, Americans may be more comfortable leaving all the nifty gadgetry to 007. ■



By 2004, biometric visas will be required for all foreign travelers entering the United States.

Top Billing

NEWS FROM INSIDE THE BELTWAY

Rep. George W. Gekas (R-Pa.) has introduced a bill mandating penalties for identity theft. The **Identity Theft Penalty Enhancement Act of 2002** (H.R. 5588) proposes that anyone who knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person shall be sentenced to two to five years in prison.

The **National Institute of Standards and Technology** (NIST) has released guidelines for the security certification and accreditation of federal information technology systems. While NIST designed the guidelines to be used by the federal government, it claims that they are applicable to all types of IT systems. The guidelines are available at www.nist.gov.

The **Organization for Economic Cooperation and Development** (OECD) has also come up with nine security guidelines that it is asking government, industry and PC users to follow. The guidelines, available at www.oecd.org, replace 1992 guidelines and suggest that all businesses factor security into the design and use of their systems and networks.

Federal Trade Commissioner Orson Swindle is asking global corporations, small businesses and the government to work together to create a "culture of security." Swindle said that security is no longer a choice but an imperative.

If the **U.S. Department of Defense** (DoD) bans the use of free open-source software, many of the DoD's workgroups defending the country against cyberattacks would experience "immediate, broad and strongly negative impacts," according to a Mitre report commissioned by the DoD.

For Washington updates, visit our website at www.csoonline.com/wonk.



Secure your entire network.

Today complete security means protecting data and voice, along with everything else your network currently includes. Having the right firewall or even securing your wireless LAN's and VPN's for data is just a starting point. With the possibility of threats like accessing stored voicemails or intercepting IP Telephony traffic looming over your network, you need complete multi-vendor, multi-technology, multi-applications security consultancy.

Protect all your points.

Introducing the Avaya Enterprise Security Practice. Our Security Consultants offer expertise in voice, data, and converged networks, with both technology and vertical certifications. Avaya helps secure internal and external points of access, including IP Telephony, Messaging and CRM, as well as VPN's, wireless LAN's and PBX's.

With communications networks now made up of multiple inter-

connected parts, it's no longer safe to just protect individual pieces of them. That's why you need Avaya, the company that can assess, develop policy and design security for your whole network.

**WHICH PART OF YOUR NETWORK IS LEAVING
YOUR BUSINESS OPEN TO BREACHES IN SECURITY?**

Ensure your company's future.

Don't leave your communications network unprotected. Prepare for today's rapid changes in network security and sign up for our Web Event at avaya.com/secure

AVAYA

COMMUNICATION WITHOUT BOUNDARIES

Securing the Network

Larry Bickner, vice president and information security officer of Nasdaq, answers readers' questions
Edited by Kathleen Carr

Q: I get a lot of script kiddies hitting our websites, apparently trying to overflow the URL buffer and access the system files. What can you tell me about this three-pronged exploit?

A: This falls into the "script list" set of hacks, where the script follows a logical progression of attacks to gain access to a target system. The problem is that there are hundreds of variations on the theme, with more coming each day. I suggest maintaining a focus on the totality of the attacks faced by your websites.

It is not unreasonable to worry about the sheer number of attempts on your systems, even though your logs suggest that they are not soaking through your defenses. You are faced with the fact that, if just one box is misconfigured and vulnerable, you will have a problem.

You need enough overlap of controls, countermeasures, monitoring and surveillance to allow you to effectively detect and stop a penetration—before it does any damage to your products or services. Given the thousands of known hacks and dozens of uncorrected vulnerabilities in the wild at any given time, you have to play a game of probabilities by stacking up solid firewall controls, standard images, religious patch management, keen intrusion detection systems (IDS) and dedicated staff against the odds.

Q: At your company, do you determine the level of protection based on data classification, or do you treat all the information as crucial? Do you have any internal process to analyze logs and try to predict hack attempts?

A: Yes and no. Rarely can you influence the sensitivity level of data. It is not clearly identifiable within the overlapping layers or network, system, application and operational controls. I keep the sensitivity or classification level in the back of my mind during risk reviews because it establishes the why of the attack equation, and I set the minimum protection level, in part, based on the sensitivity and value of the information.

We all have to deal with the fact that, in the end, we cannot accurately predict when someone will start attacking our internal or external systems or net-

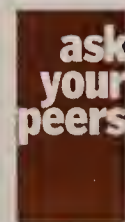
works. Looking through megabytes of logs is unlikely to yield a good enough answer to justify the time and tool costs involved. I prefer to rely on some level of intuition that is based on external threat levels identified across our industry and across the Internet, the internal climate within my company, the state of vulnerabilities, the availability of hacking tools and methods, and last but not least the trends information from our IDS and other surveillance systems. From this amalgam of knowledge and information, we attempt to set our risk level on a weekly basis and increase our protective condition level to match.

Q: During the past few years, outsourcing of information security services has been growing. What is your opinion of outsourcing those functions in the financial services industry, and what, if any, information security services would you suggest outsourcing?

A: It seems that outsourcing is an organizational process that cycles through companies, and now, in a down economy, the outsourcing of security services is a topic of conversation. Gaining real cost advantage in any outsourcing deal is the relative difference between your internal cost of various security services and cost for delivered and comparable services from a contractor. In situations where the gap is wide, due to internal issues (for example, the inability to train and keep key staff), and where the industry has commodified the service (for example, good quality at low cost and defined metrics for performance), outsourcing is a clear winner.

The other issue is one of trust; you can outsource security services only to contractors that you trust as much or more than your internal staff, and while contract terms can establish this foundation, each security manager has to determine his level of comfort. Areas in which I would look for outsourcing opportunities include IDS management, penetration testing, training and awareness materials development, and product certification. ■

Larry Bickner is vice president and information security officer at Nasdaq.



Have a security topic to suggest or an expert you'd like to hear from? Send your thoughts to Assistant Managing Editor Kathleen Carr at kcarr@cxo.com. To read more on securing your network, go to www.csoonline.com/counsel.



tyco / Fire & Security



SYSTEMS •

SOLUTIONS •

SERVICE •

CONFIDENCE •

Fire

Safety

Theft

Workplace Violence

Information Loss

Employee Backgrounds

Surveillance

Access Control

Risk Liability

Bio-Terrorism

Unspecified Threats

ARE YOU STILL RELYING ON TRADITIONAL SECURITY?

The world has changed. As security professionals, we now have to be prepared for anything, including the unspecified and the unthinkable. It's an enormous responsibility, but one that doesn't have to be yours alone. We understand how your job is more important now than ever before, and we want to help. Let us get to know your business and your concerns. Then we'll draw from the broadest range of products and experience available, including the latest in digital video and access control. All to create a solution that meets the unique security needs of your company. Getting in touch is easy. Just call us at **1-877-258-6424** or visit adt.com. And when everybody looks to you for peace of mind, look to us. **ADT. Always there.**

Is the Sky Really Falling?

A CSO who spreads security paranoia is only making his own job harder
By David H. Holtzman

THE SQUEAKY WHEEL doesn't always get the grease. Sometimes it gets replaced." This fortune cookie quote nicely sums up the career cycles of security professionals. Even in the most well-oiled corporate machine, the security officer may sometimes feel compelled to sound an alarm when the security pressure gets hot enough. That leads to friction with other executives who view crash-and-burn stories as a cynical attempt by the CSO to extort an increased budget or make a political landgrab. Sometimes it is. So what's the sometimes panicked CSO to do?

Avoid the temptation to be an alarmist. It's true that many security professionals have developed a taste for hyperbole. Becoming an alarmist is an occupational hazard of the security profession because it does work (at least at first). Like other targets of scare tactics though, the victims will eventually build up a tolerance to these The Sky Is Falling warnings. I call these Chicken Little speeches. I've also heard them referred to as FUD (Fear, Uncertainty and Doubt). Unfortunately, dropping the melodrama often means losing the funding for a fix and necessitates a compensatory strategy. The challenge for you is to get attention in a nonvolatile yet effective way.

Treat security like a business. A better approach to handling the P&L types is to beat them at their own game by presenting security as a business decision instead of an all-or-nothing dogma. Frame the discussion around the company's capacity to absorb risk versus the increased cost of doing business. This encourages management to emotionally consider the downside before a problem ever happens and, more important, creates a buy-in for the resulting decision.

Create a measurement scheme. Experienced businesspeople manage to the deltas (variance from an expected number), not to absolute numbers. That works as well for security as it does for sales, headcount or network bandwidth. Modeling security by showing risk on a color-coded chart or on a numeric yardstick hides the distracting detail while highlighting the key business drivers and foreshadowing the dangers.

Manage expectations. The range of choices should be calibrated to best practices

in the company's business area. Banks should have more intense computer security than say, car dealers. That's just common sense; but if you ask the managers of both businesses how much security they want, they want it all—that is, until they see the price tag. Providing industry standard comparisons is an important piece for setting up a comfort zone for decision making.

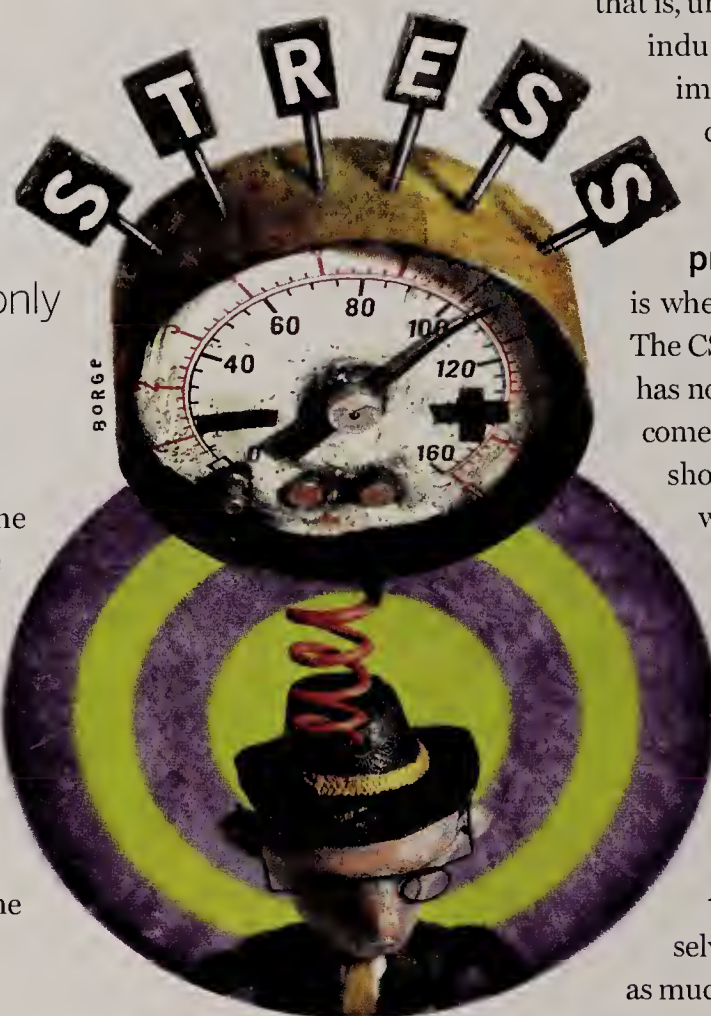
Provide regular feedback on progress of security goals. This is where measurement comes in handy. The CSO can even report on areas that he has no control over (which, of course, becomes a form of control). The emphasis should not be on "tattling" but on how well the company is doing against its own goals.

Recommend just enough security. Too much security is disruptive. Department heads like to ask for more than they need so they end up getting what they really want. Security officers that haggle like this are setting themselves up for a credibility problem just as much as the alarmists are.

Avoid "trust me" arguments. Chicken Little talk is counterproductive because it forces management to treat security as an either-or proposition instead of as a wide range of choices. Since most executives don't have enough experience to make a judgment, they are forced to rely on the security officer's appraisal of the risks. This reduces the tough problems down to: "Do I have confidence in the security guy?" As tempting as it is to be an authority figure and cut through the discussion with a pronouncement, it's just not a smart career move.

What's in it for the CSO? At a minimum, job longevity. Ideally, it leads to a more harmonious and less stressful work environment. When security people stop resorting to voodoo mumbo jumbo to scare up what they want, they'll spend less time worrying about getting stuck. Life for the chief security officer will be a lot calmer if a problem never becomes a crisis and if the solution doesn't require the blood of a sacrificial chicken. ■

David H. Holtzman, former CTO of Network Solutions, also worked as a cryptographic analyst with the U.S. Navy and an intelligence analyst at DEFSMAC. He can be reached at david@globalpov.com. Send feedback and column ideas to Senior Editor Daintry Duffy at dduffy@cxo.com.



MERGER
PLANS

IBM

BIG KAHUNA

BIG CHEESE

BIG MOUTH

Tivoli software

SECURITY MANAGEMENT PLAY

- 1] WIN WITH SECURITY: It isn't always about hackers. e-business security must also ensure that only the right users (within and outside of your company) get the right information at the right time.
- 2] WIN WITH TIVOLI: Whether it's granting access to customers or CEOs on PDAs, Tivoli Security Management software centrally secures and manages your network across multiple platforms. Tivoli. Part of our software portfolio including DB2®, Lotus® and WebSphere®.
- 3] MAKE THE PLAY: Visit **ibm.com/tivoli/secure** for a white paper on how Tivoli Security Management can maximize your ROI.

@business is the game. Play to win.™

IBM, Lotus, WebSphere, the e-business logo and e-business is the game. Play to win are registered trademarks or trademarks of International Business Machines Corporation in the United States and other countries. ©2002 IBM Corporation. All rights reserved.

SPECIAL REPORT

Risk: A Whole New Game

ECONOMICS IS CHANGING INFORMATION SECURITY. YOU CAN HELP
WRITE THE NEW RULE BOOK. BY SARAH D. SCALET

IN THE WORLD OF BUSINESS, RISK—FOR ALL ITS UNCERTAINTY—HAS A RULE BOOK. IN FACT, THE FINANCIAL AND INSURANCE INDUSTRIES HAVE BUILT AN ENTIRE DISCIPLINE AROUND PREDICTING THE chance of an injury or loss, protecting against it and reaping the benefits if bad things never happen.

The rules are the principles behind risk management, and they're fueled by the raw data of financial statements from public companies, complex actuarial tables of past events and decades of academic rigor.

Information security, however, is a whole new game in which the economic goal is clear: Spend the smallest amount of money necessary to protect the enterprise. Win in a photo finish.

But how? Companies have a hard enough time counting how many dimes they're spending to protect how many dollars, never mind calculating the damage from an employee who inadvertently (or not) reveals company secrets or the value of the training that might prevent such an occurrence.

Security's only reward—if you could call it that—is that weaker competitors are often the ones plagued by such mistakes and miscreants. But because companies are reluctant to talk about either their best practices or their breaches, it's hard to know exactly where the competition stands. With numbers fuzzy and the payoff vague—*nothing bad happened to us today, thanks*—risk management in information security has traditionally had a different meaning than it does for the rest of the business community.

But all that is about to change.

As information security—and along with it the CSO—rises in prominence, so too does the need for practitioners to apply traditional theories and models of risk manage-

ment to information security—to put structure around the process of mitigating risks, accepting some of them and transferring others to third parties.

"If you don't manage risk you're going to lose money," says Steve Katz, former CISO for Merrill Lynch, Citigroup and J.P. Morgan who's now a consultant. "Companies have been great about looking at credit risk or the risks of a particular customer or region. Companies and regulators are simultaneously beginning to realize the importance of operational risk and information secu-

In our guide on **HOW TO WIN AT RISK**, you'll find:

Reasons—and formulas—for calculating a security ROI in **Calculated Risk** (Page 30).

A look **Inside the Sausage Factory** of security budget surveys (Page 38).

Adding up the costs when you learn the hard way that **It's Not Easy Being Breached** (Page 40).

An economist's viewpoint on security and **The Art of Uncertainty** (Page 44).

How cyberinsurance puts **Safety at a Premium** (Page 50).



rity as a component of it.”

Right now, several factors are converging to make this, the economics of risk, *the* issue for CSOs in 2003. Companies offering cyberinsurance are creating actuarial models—rather than guesstimates—that map security practices to financial losses. They’ll soon be helped along by the new Basel Capital Accord (see “Safety at a Premium,” Page 50), which will establish ways for financial services companies to measure operational risks. Courts are starting to apply dollar signs to losses from security breaches. Legal precedents and emerging standards will make it easier to quantify exactly when companies have done enough.

Meanwhile, CEOs and CFOs are demanding accountability for every dollar spent, providing new incentives for CSOs—and security vendors, analysts and consultancies as well—

to help prove themselves worthwhile. As a result, companies are starting to calculate a return on security investment, based primarily on the cost of security, the cost of breach and the probability that it will happen.

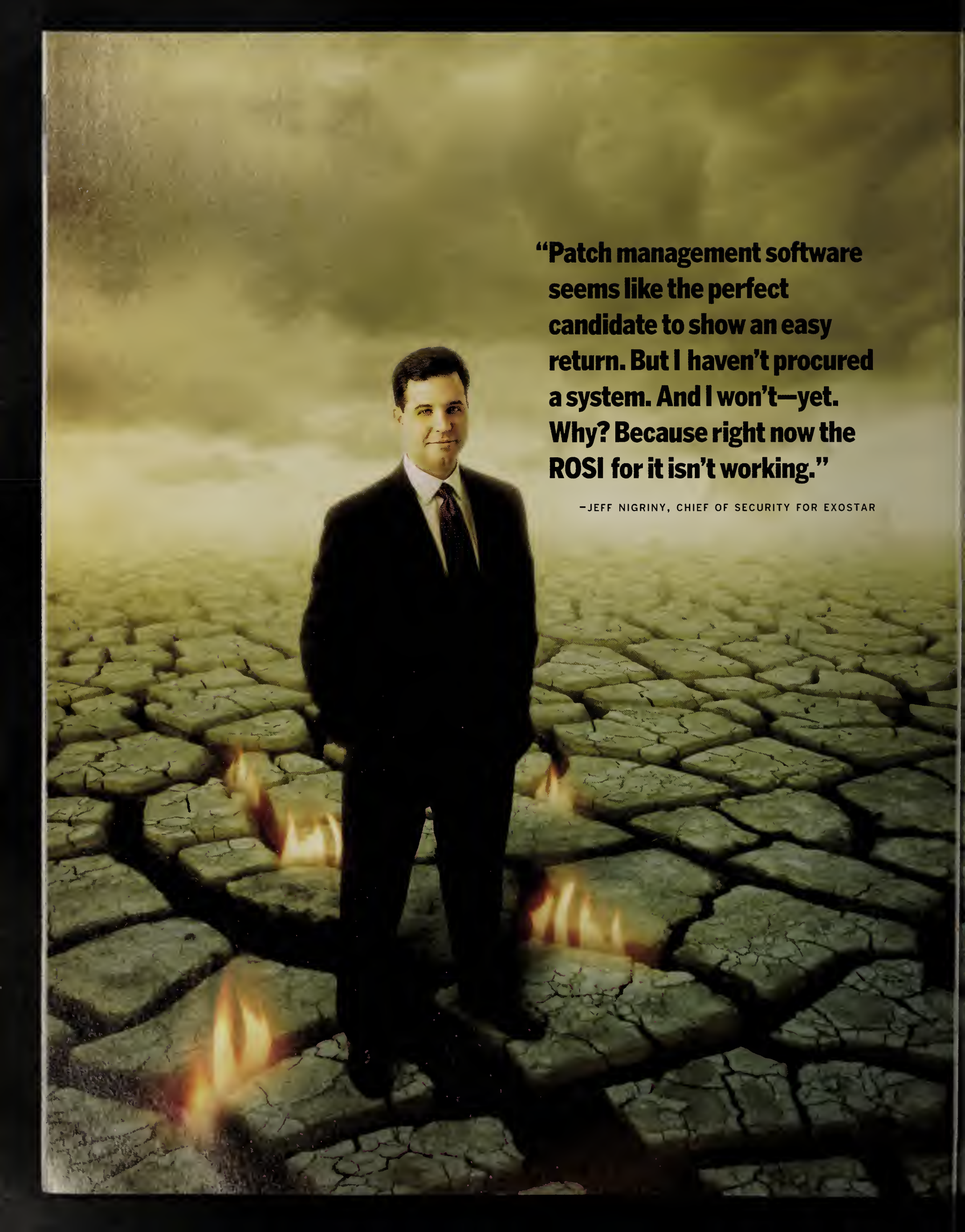
It would be naive at best to suggest that any of this is a science. “We’re just leaving puberty,” is how Katz describes the field of information security. Far from knowing the *answers* about how much money to spend and where to spend it, we’re just starting to know the *questions*.

But one thing is certain: In the coming years, the information security community has the chance to work with auditors, economists, accountants, lawyers, insurance companies and a bevy of other experts to find ways to put structure around the money spent on information security. The ability to join in this

dialogue is vital to individual CSOs and the burgeoning professional as a whole. But, to hear at least one observer tell it, the convergence of risk management and information security might have even greater implications.

“I think this is going to make or break the economy,” says Thomas Koulopoulos, president, CEO and founder of the Delphi Group. “Unless we can find a way to more securely—and with greater trust—transact across enterprise lines, I don’t think we’re going to have the economic growth everyone is hoping for. I think this is fundamental to growing—and I hate to use this phrase—*a new economy*, if there is a new economy out there.”

For your business and profession to survive, you have to play the game of risk. If you want to win, then help write the rules. We’ll help you get started. ■

A man in a dark suit and tie stands in the center of the frame. He is looking directly at the camera with a slight smile. The ground he is standing on is composed of large, irregular, cracked stones, resembling a dry, cracked earth or a volcanic surface. Several bright, orange and yellow flames are rising from the cracks in the stones around him. The background is a hazy, yellowish-brown sky, suggesting a smoky or dusty atmosphere. The overall tone is dramatic and somewhat ominous.

“Patch management software seems like the perfect candidate to show an easy return. But I haven’t procured a system. And I won’t—yet. Why? Because right now the ROI for it isn’t working.”

—JEFF NIGRINY, CHIEF OF SECURITY FOR EXOSTAR



Calculated Risk

SURE, DETERMINING AN ROI FOR SECURITY IS DIFFICULT. BUT IT'S ALSO THE KEY TO SELLING YOUR BUDGET. HERE'S OUR THREE-STEP GUIDE TO GETTING STARTED.

BY SCOTT BERINATO

JEFF NIGRINY WANTS TO BELIEVE THAT PATCH MANAGEMENT SOFTWARE IS A GOOD INVESTMENT. BUT HE CAN'T. UNTIL NIGRINY, CHIEF OF SECURITY FOR AEROSPACE AND DEFENSE SUPPLY CHAIN

exchange network Exostar, can *prove* a positive return on his security investment, or ROSI, he will continue to manually patch systems. He will download the patches, perform regression testing, deploy them in a staging area, determine what machines need patches and then, finally, spit them out onto his network.

"Patch management software seems like the perfect candidate to show an easy return," says Nigriny. "Everyone kind of feels like it's the right thing to do. But I haven't procured a system. And I won't—yet. Why? Because right now the ROSI for it isn't working."

He calls this particular scenario "the most difficult and abstract in terms of risk and return" that he's worked on. It's nothing like 24/7 monitoring, which he said was a cinch to bring to the brass, especially since after he proved an ROSI for monitoring, he also showed that he could cut costs *another* threefold by outsourcing it.

But with patching, he continues to build and then rebuild his ROSI models, looking for that elusive positive return, all the while fixing his systems the old-fashioned way.

Many of you might be snickering by now

because you don't share Nigriny's idealism about the necessity of an ROSI to sell security to the CEO and CFO. In fact, it seems you are legion in your resistance.

It's understandable, in a way. As CISO Tina LaCroix of insurance broker and consultancy Aon points out, "This elusive packaging of the ROI formula to validate our existence is one that may take us down an endless path," a path that probably looks to many CSOs like the one Nigriny's put himself on now with patch management.

But, in fact, it's not an endless path, and we're here to suggest not only that you *can* use ROSI to sell security internally but that you *must*. As good a reason as any for the mandate is this: Economist Frank Bernhard's research shows about six cents of every *revenue* dollar is at risk due to a lack of information security, whereas many companies spend barely a dime of their *IT* dollar on security.

"I'm not sure why IT tends to disregard these tools; it's a bit frustrating to keep hearing you can't do it accurately," says Bob Jacobson, founder and president of International Security Technology (IST), which handles physical and logical security risk assessment. "It's not true. The tools are there. Nuclear uses them. Pharma uses them. The whole world has used ROI in security for a long time. [CSOs] have an opportunity to make a major contribution in their organization, if they have the willingness to learn this."

None of which is to say ROSI isn't hard work for a security executive; it is. But it's not hard like calculus—plenty of researchers and economists have taken care of sigmas and mus and other

■ **IN THIS STORY:**

Find the data you need to calculate a security ROI
■ Learn the basic math to do it



Check Point.
We secure the networks
of the Fortune 500.



As the world leader in Internet security, Check Point's™ integrated security solutions Connect, Protect, Manage and Accelerate the network security of more than 100 million users worldwide.

CONNECT. Leading global companies rely on Check Point VPN solutions to connect employees and offices everywhere. Regardless of where business happens—even in the most remote locations—people and companies are securely connected to their critical information.

PROTECT. Check Point's fail-safe firewall infrastructure provides the highest level of security for every network from the edge to the core. Our authentication, access control, and content security features have become the trusted global industry standard.

MANAGE. Check Point's revolutionary Security Management Architecture (SMART™) lets you instantly deploy and distribute security policies regardless of user location. All aspects of network security can be defined and managed from a single console dramatically reducing your total cost of ownership.

ACCELERATE. Check Point's VPN and firewall solutions deliver wire-speed performance up to three times faster than other network solutions. Now you can maintain absolute network security without sacrificing the performance of business-critical applications or bogging down your network.

Find out the latest in Internet security by downloading our white paper "Building Secure Wireless LANs" at www.checkpoint.com/wireless/cso or call (866) 488-6686.



We Secure the Internet.

esoteric economic math already. It's hard like running a marathon—ROSI requires legwork, and lots of it.

We'll set you on the path to succeed in building and using ROSI as a tool to sell security, with a simple three-step primer. Trust us, your CEO will think it's worth it.

STEP 1: RETHINK YOUR ASSUMPTIONS

Exostar's Nigriny is clearly not in the majority when it comes to security professionals and ROSI. The defeatist shrugs that accompany conversations about ROSI have become conventional wisdom. "Most execs want hard numbers to make financial decisions, and we live in a world where you can't always have that," says Rich Mogull, research director at Gartner G2 Cross-Industry Research. "I mean, what's the ROI of a fire extinguisher?"

According to one study the American Society of Safety Engineers (ASSE) cites, the ROI of fire extinguishers is in fact about a \$3 return for every \$1 invested if you take fire extinguishers as part of a larger corporate health and safety initiative—which you should, since fire extinguishers (like IT security) rarely show up as a discrete security purchase. (For the sake of our argument, ignore that Mogull's example is hamstrung by the fact that, often, regulation mandates fire extinguishers.)

The point here is ROSI can be calculated and is being calculated. To do so with information security, though, there needs to be a deliberate effort to rethink some of the industry's assumptions and cultural biases. Specifically, there are two biases that need to be eliminated:

PRECISION IS NOT THE GOAL. One of the reasons that ROSI might feel like an endless path comes from the fact that there has been a natural tendency in the tech sector toward approaching problems with the precision a software engineer would expect. The "hard numbers" Mogull assumes are required.

"This is a classic problem that technologists have," says Kevin Soo Hoo, a researcher at security consultancy @Stake doing ROSI studies, and who at Stanford University wrote his thesis, dense with economic theory, on the subject. "They don't understand that you can make rough guesses to work out a problem. We dive into an ROSI study, and the engi-

neers are focused on the minutiae and want to argue for days whether some variable should be .6 or .55. It doesn't matter," Soo Hoo says emphatically, as if he's been through this more than a few times. "Choose one!"

With ROSI, like all risk assessment, the goal instead needs to be *accuracy*, which isn't at all the same thing as *precision*. Notice that the ASSE study suggested about \$3 for every \$1. There was no attempt here to delineate the exact return, because that's not the point. The point is to provide a set of guiding principles from which you, your CEO and CFO can make good decisions about what's acceptable. In other words, the CEO doesn't (or shouldn't) care if a return is precisely \$3.13 for every \$1 spent or \$2.97. He cares that it's accurate to suggest about a 3-to-1 return, and not a 1-to-1 return or, worse, a 1-to-3 return.

THE DOGMATIC I.T. MIND-SET MUST BE ELIMINATED. It's obvious why IT tends to approach problems with binary thinking. It is, after all, the language of the trade. But an on-off, "either we've been hacked or we haven't" view of the problem will make ROSI an impossible task. (Some believe it helps to eliminate binary terms from their discussions so that *security* becomes *risk management* and threats aren't *eliminated*, they're *mitigated* and so forth.)

Back to the fire extinguishers. A binary thinker might suggest that, since there was no fire last year, there was no ROSI. If that is the attitude at your company, it's time to initiate some awareness and education because that's not how risk mitigation works. Think of it this way: If you wear your seat belt but don't get in a car accident, does that mean you ought not invest in a seat belt because there was no return?

No. You did get a return, because return is not measured in a dogmatic world of what did or did not occur, but in the stochastic world of what might occur and how likely it is to occur. That is the game of risk; prepare for something to happen by investing in ways to stop it from happening.

"You can't get from the cost of security incidents directly to a return on investment," says Thomas Koulopoulos, president, CEO and founder of Delphi Group, an information technology research and consulting company. "You need to focus on the intermediate step. The probability."

STEP 2: DO THE LEGWORK

Here's just a portion of the effort Nigriny put into his patch management ROSI: "I am throwing into it how many patches per year I apply, based on three years of data. I sit down with the network team and talk about the types of patches, their criticality level. I look at how long it takes to vet the patch. How many rollouts result in a rollback because of problems with the patch. Then I look at how many patches I *should* have installed, based on all the patches on all the mailing lists I subscribe to. I dedicate a day to that, but I could take weeks. Eventually, I come up with total time I was at X-percentage risk level before the patches were installed. Here's the average cost of an incident to us; that's my baseline number. You absolutely have to have that. There are industry baselines for this you can find. You can talk to peers at other companies about their baselines and massage them for your situation."

You get the idea. ROSI is labor-intensive. In his partial history of the patch management ROSI above, though, Nigriny demonstrates much of what you need to do to prepare to use ROSI. Here it is:

FIND AND USE DATA THAT'S OUT THERE. The most common misconception CSOs have about ROSI is that there isn't any data available to even start an ROSI study. There's a ton of it, and the body of usable statistics is growing. Some is free for the taking, other data you might have to pay for, but the actuarial figures do exist. (CSOs who come from a physical security world probably know this, as they've dealt with risk of theft, natural disasters and so forth for a long time and have sought out the data on the probability of such events.)

CERT and Riptech, for example, have combed over data to discover some incredibly useful facts. They measured attacks per company, which right now come in at a rate of 2,112 attacks over two years. What's more, at current growth, that number will grow to 8,403 attacks per company over two years. That's a fourfold increase—which strengthens the ROI argument. Mitigation now will protect against a growing threat. In addition, CERT built some complicated math that shows security spending is a diminishing-return game; that is, as you spend more, the probability of attack goes down but at an ever-



slowing rate. By crossing this data with what are called indifference curves (too complicated to get into here), you can actually determine a kind of sweet spot of security spending for your organization.

Consultancy @Stake has published well-known numbers that prove that the earlier you build security into applications, the higher the return. The company's researchers now believe they probably lowballed their 21 percent ROI for incorporating security from the start.

You need to cull as much of this kind of data as possible and keep it in your toolbox because the more you set out to show returns on security, the more you'll be coming back to these kinds of figures.

CANVASS TO GET WHAT'S NOT OUT THERE. If the first piece of advice is "go to the library," then this is "play detective." You must develop certain numbers, like the cost of incidents to your organization and the probability that a given incident will occur. While these numbers can be based on research, to hone them for your situation requires canvassing of the relevant players—including business managers within your company, peers at similar companies, economists, consultants and so on.

"My experience is that the business man-

agers have clear ideas about loss, risk and what it will cost them and probably more experience than the security guys know," says Jacobson of IST. "You have to go to Mr. Jones and ask him what it would cost him to be down, what is his optimum recovery time. He will have better answers than you think, especially as he thinks about it more."

KNOW THYSELF. With all of this data in hand, you can start to build a threat profile. You'll need to know the threats specific to your industry, the probabilities of certain types of attacks based on the kind of company you have or the kind of infrastructure you use. Crude but true example: Financial services companies face more attacks than manufacturing companies. Companies in the news endure spikes in attempted incidents. The Riptech statistics actually do some demographic breakdowns based on industry sector.

CALCULATE CONSERVATIVELY. We're moving from how and where to get data to how you're going to present it. When pulling together numbers for a ROSI study, always play it safe. Don't assume costs or benefits you're not sure of. If someone says the probability of an attack is between 10 percent and 20 percent, use 20 percent. If they say the cost of an attack is

\$50,000 to \$100,000, take the bigger number.

And use "soft returns" as gravy. Soft returns are generally the hardest elements of a security investment to quantify. An improved brand image due to increased security is a soft return. Trying to add these to the equation is difficult—some skeptical CFOs might even dismiss your ROSI argument as "fudged" because of these variables. Therefore, soft returns are more effectively used as an added benefit on top of ROSI when selling executives.

KNOW YOUR AUDIENCE. And when selling the bosses, the CSO should learn what those executives are looking for in terms of return. "I can't tell you how many times these things are rejected out of hand, because IT is selling something that the executives aren't even looking to buy," says Delphi's Koulopoulos.

Know how the executives want the ROSI positioned—cash savings, productivity gains, increase in security—and move forward that way. Many sources also report that making the ROSI case interactive for executives—allowing them to tweak variables and watch what happens to the ROSI—is by far the single most effective selling tool you can use. "The key is not to be defensive about the data, as I think IT sometimes can be," IST's Jacob-

son says. "Don't defend the model; explain it."

Nigriny thinks there are other, underrated sales skills CSOs need to foster in themselves. A general familiarity with accounting is priceless, he says. Also, "You have to be good at public speaking and at PowerPoint engineering. If you're speaking to the CFO, expect him to do some number crunching; have your numbers ready for him. The CEO? The executive summary is far more important. Talk to the CFO ahead of time; you'll have his support, and the CEO won't have to sit through the numbers discussion," says Nigriny.

We weren't kidding when we said this is laborious, intensive work. To Nigriny, ROSI is fractallike, in that the closer he examines his situation, the more intricate it becomes. "Every time I thought I had it covered, a raft of new variables came up. I've just got this swag of numbers here I have to deal with," a nonplussed Nigriny says.

It's up to the CSO to set the thresholds of what's really needed for a particular scenario. You can make ROSI as simple or as complicated as you think is necessary, and an obvious tenet that emerges is that a simpler ROSI will be somewhat less accurate than a detailed ROSI, but the detailed version will require ever more legwork.

STEP 3: DO THE MATH

In the end, the math is simple. You subtract cost from benefits. A positive number is good: a return on investment. A negative number is bad: You're spending more than you're getting.

Of course, the math behind the variables and coefficients that go into the costs and benefits is massively complex. Fortunately, if you've got raw data from your legwork, someone else has done or will do the difficult computations for you. Still, there are some basic risk computations you should know. Here they are:

ANNUAL LOSS EXPECTANCY. ALE is the foundation of risk assessment. It is what it sounds like: how much money you expect to lose per year due to some sort of security incident. Note that this is different than the raw cost of an incident (which, remember, you should always keep as a baseline). It's actually the raw cost times the probability of an event in the next year. So the ALE of a security breach that costs \$1 million and has a 40 percent chance of happening is:

$$\text{Incident cost} \times \text{Probability of incident} = \text{ALE}$$

$$\text{\$1,000,000} \times 0.4 = \text{\$400,000}$$

MODIFIED ALE. mALE is the same equation, but with the probability affected by mitigation measures you take. Imagine the above scenario were a virus attack. You introduce antivirus software that cuts in half the probability of a successful attack, to 20 percent. Or, you start an awareness program that reduces probability 5 percent. (These are arbitrary, but if you've done the legwork from Step 2, you'll have real numbers to plug in here.) Then:

$$\text{Probability} \times \text{Mitigation A} = \text{Modified probability}$$

$$\text{Probability} \times \text{Mitigation B} = \text{Modified probability}$$

$$\text{A: } 0.4 \times 0.5 = 0.2$$

$$\text{B: } 0.4 \times 0.95 = 0.38$$

You must consider each mitigation separately. Once you've gone through the process for several types of mitigation, you can pick which ones you feel are most important or provide the best return. (Of course, some mitigation measures will have overlapping effects. We're not putting that into this math.)

At any rate, adding mitigation measures produces modified ALEs:

$$\text{Incident cost} \times \text{Modified probability} = \text{mALE}$$

$$\text{A: } \text{\$1,000,000} \times 0.2 = \text{\$200,000}$$

$$\text{B: } \text{\$1,000,000} \times 0.38 = \text{\$380,000}$$

So, in each case you've reduced your ALE.

$$\text{ALE} - \text{mALE} = \text{Savings}$$

$$\text{A: } \text{\$400,000} - \text{\$200,000} = \text{\$200,000}$$

$$\text{B: } \text{\$400,000} - \text{\$380,000} = \text{\$20,000}$$

This is the step at which executives will want to interact with the model, seeing how different measures that they take affect their mALE.

Now, to get a basic return, you simply subtract the cost to implement each mitigation measure from your savings on your mALE by implementing the mitigation. Let's say mitigation A, antivirus software, costs \$120,000. And mitigation B, an awareness program, costs \$8,000. Then:

$$\text{Savings} - \text{Mitigation cost} = \text{ROSI}$$

$$\text{A: } \text{\$200,000} - \text{\$120,000} = \text{\$80,000}$$

$$\text{B: } \text{\$20,000} - \text{\$8,000} = \text{\$12,000}$$

Both mitigation measures provide a ROSI (if the final number came out negative, then you're spending more than you're getting back). Awareness actually has a higher return; or put another way, you get the most bang for the buck. (Your savings are 2.5 times what you spend, whereas in the antivirus case, they are 1.7 times what you spend.)

This is a simple model. No doubt CSOs, consultants and vendors with their own ideas will hue and cry that we've presented ROSI in *this* particular, facile way. But we're only trying to provide a guiding primer. To attempt more in this space would be a fool's errand. (For example, we didn't even approach the concept of Net Present Value, which takes into account costs and benefits over time as if all the money were here now. Ask your CFO.)

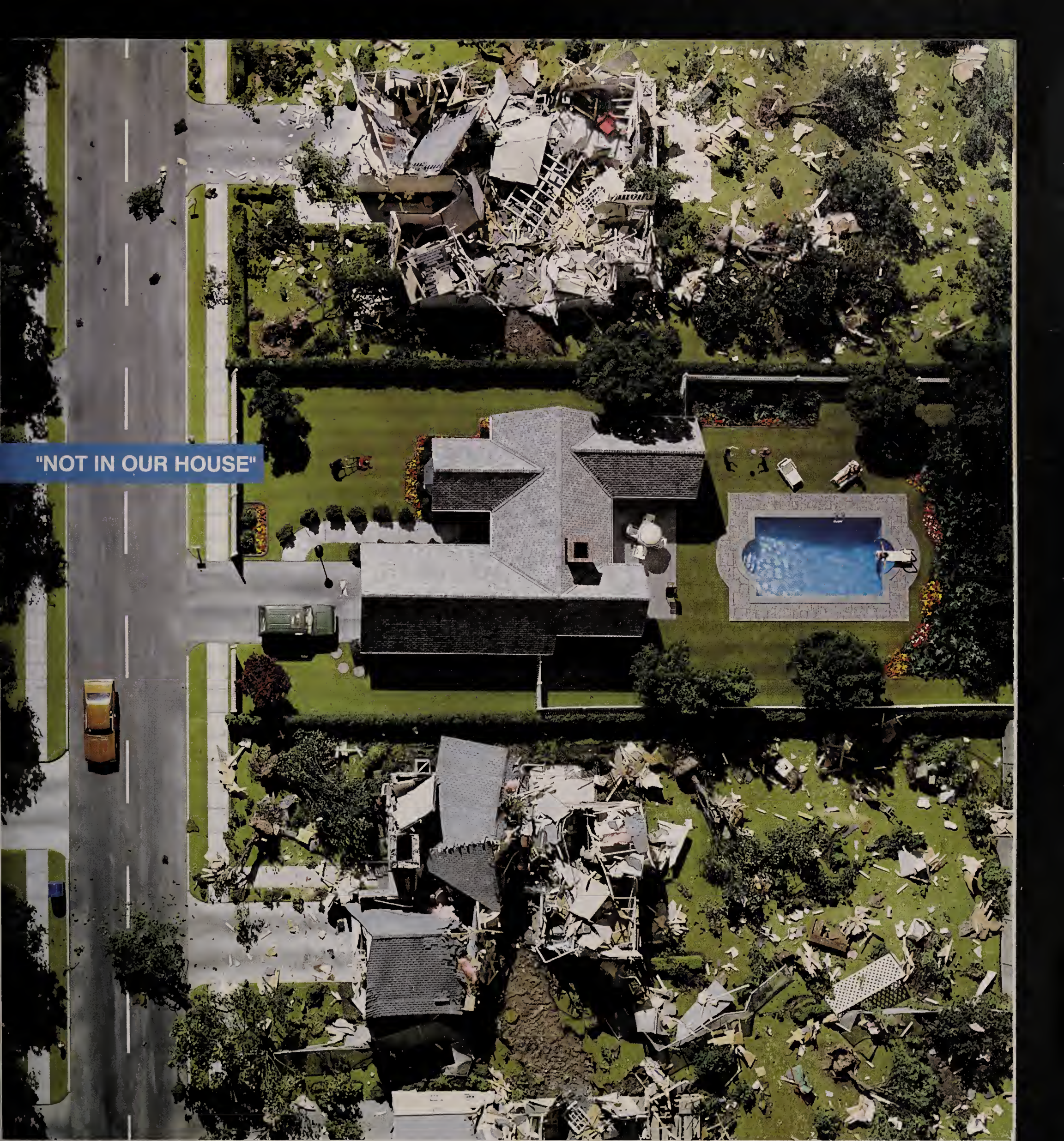
Don't take this as a final "how to" but rather as a starting point to develop your own ROSI. But don't forget: The most important message is to do the homework. Collect as much data as possible so that there's plenty to crunch.

ROSI is empirical, but in many ways it's emotional, believe it or not. It is about coming up with numbers, but those numbers are only useful in the context of how executives *feel* about them. ROSI is risk economics that paints a picture of your organization's attitude toward security. What level of risk is the enterprise comfortable with? How does the company prioritize its limited resources? Is technology or awareness more valuable as a tool? Suddenly you're answering business questions based on the security numbers.

"The numbers right now show patch management automation doesn't provide a positive return for this organization," Nigriny says. "So why would I do it? It just doesn't make sense." Just by coincidence, it seems, ROSI has aligned Nigriny with the business. ■

Senior Writer Scott Berinato can be reached at sberinato@cxo.com.

Security spending is on the rise, thanks in part to positive ROSI calculations. By 2003, Meta Group expects 55 percent of companies to be budgeting at least 5 percent of their IT spending on security. Read **SECURITY SPENDING GETS BOOST** for the details. Go online to www.csoonline.com/printlinks.



"NOT IN OUR HOUSE"

OKENA

Why just detect intrusions when you can prevent them?
OKENA StormWatch stops attacks dead in their tracks.
Intrusion Prevention: Security Without Signatures.



STORMWATCH

www.OKENA.com



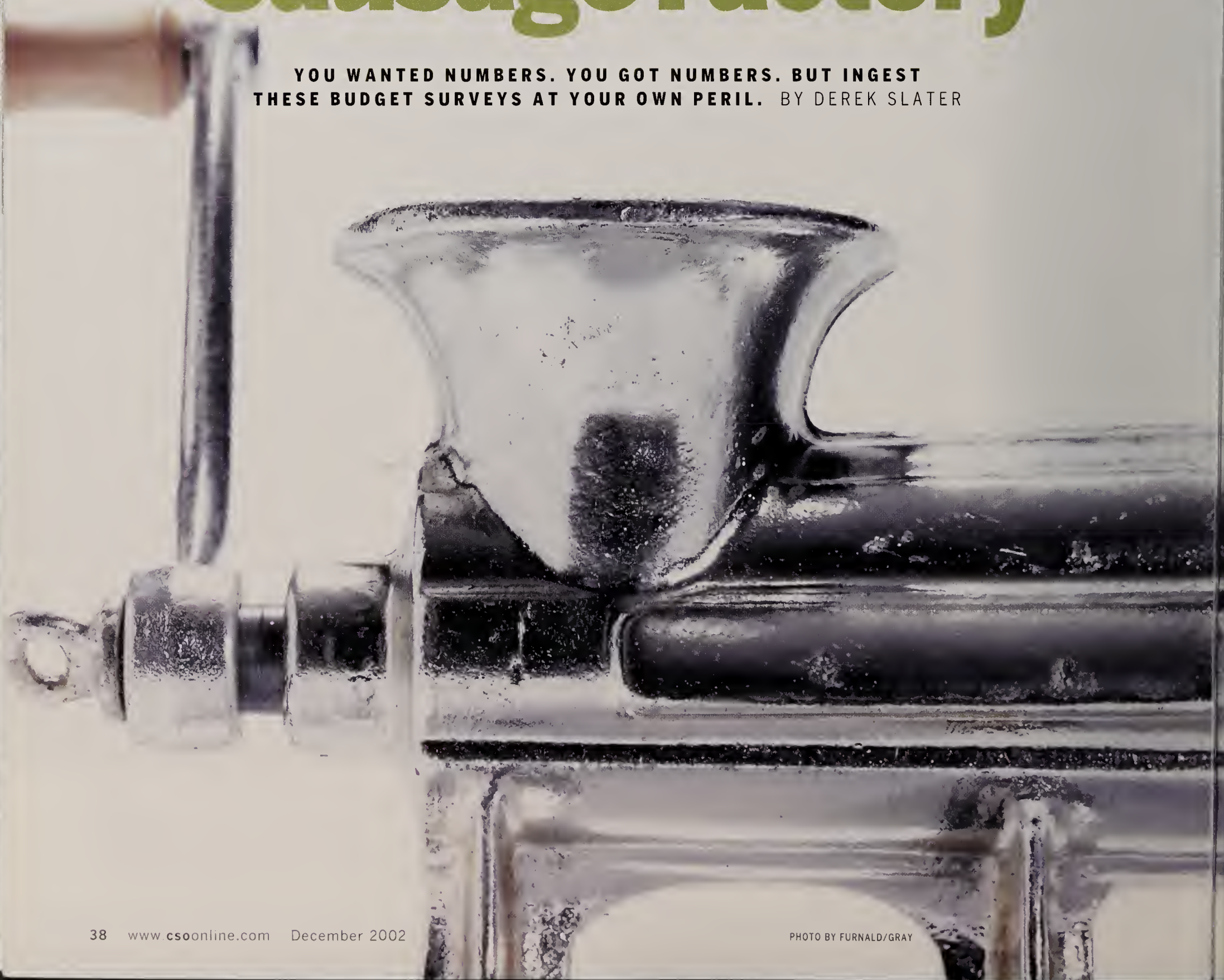
How
to Win
at Risk



SPECIAL REPORT

Inside the Sausage Factory

YOU WANTED NUMBERS. YOU GOT NUMBERS. BUT INGEST
THESE BUDGET SURVEYS AT YOUR OWN PERIL. BY DEREK SLATER



INFORMATION SECURITY IS OFTEN CALLED A "GRUDGE SPEND." CEOs ARE RELUCTANT TO SPILL HARD-EARNED DUCATS ON SECURITY BECAUSE IT'S NOT

seen as a value-added expenditure. Yet CSOs fret that they're not spending enough to secure the enterprise—and nobody knows what "enough" really means, anyway.

So a typical strategy in the budget-setting process is to eyeball your neighbors' plans to see how much they're spending. Just to make sure you're in the right ballpark.

So you want numbers? We got numbers. Gleaned from a security spending survey of 276 CIOs and IT executives, these figures line up pretty well with conventional wisdom. Consultant Karen Avery of Booz, Allen & Hamilton advises security spending should constitute between 5 percent and 8 percent of the IT budget, and our respondents clocked in at an average of 7.2 percent.

But use these numbers at your own peril because CSOs say rough benchmarks of this sort offer a very false sense of, well, security.

There are two reasons for that. First, survey numbers suffer from the sausage effect: You just don't know what's in there. Companies vary greatly in what they include in

the security budget proper. How do you account for IT staff whose duties include security along with other tasks? What about e-mail training for new employees? Your company may have a clear sense of how to answer those questions, but it's unlikely to match the policies of a majority of respondents in any given survey. Andy Reeder, CSO of Central DuPage Health, says that in some organizations even basic security items like firewalls and antivirus aren't part of the security budget. "The security office may help manage those things, but they're budgeted and implemented through the IT operational arm," he says. "It's a judgment call."

Many organizations, in fact, don't even craft a separate security budget. Steve Akridge had one of the more frustrating setups as CISO of the Georgia Technology Authority (GTA): The state senate approved a specific allocation for information security, but the money was then rolled into the GTA's IS budget. "I had to lobby the CIO to get access to money that had already been approved by the state," he says.

Another problem is that, unless you're looking at an incredibly detailed survey of best practices companies, you don't know how effectively, or appropriately, the respondents are spending their cash. "I read somewhere that the average infosecurity spending this year was 12 percent of the IT

budget. But it's all so highly dependent on what you're doing as a company," Akridge says. He describes a formal sequence for building an appropriate information security plan and says many companies fail to follow the necessary steps.

Akridge's process starts with high-level questions about what data is most important to your company, what regulations affect your company's security policies, which architecture will provide the right level of security for the right data and so forth. Some organizations may be throwing a fair amount of money at shoring up their defensive perimeter, but technology decisions like that "should be way downstream," Akridge says. If the company hasn't answered the high-level questions, "it's wasted money." Case in point: A report by the White House Office of Management and Budget found no correlation between the amount of money a federal agency spent on security and its effectiveness.

So what's the value of knowing "average" infosecurity spending? It may help a CSO defend his budget in a PowerPoint presentation, but for the purpose of figuring out whether security is appropriate, "I don't think it's of any value at all," Akridge says. To set correct spending levels, CSOs must dig deeper and look harder at cost-justification techniques. ■

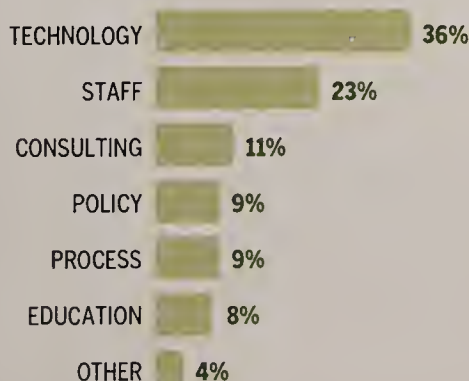
Numbers to Chew on...

7.2%

AVERAGE PERCENTAGE OF TODAY'S I.T. BUDGETS ALLOCATED TO INFORMATION SECURITY

HIGH ROLLERS: FINANCE, HIGH-TECH
TIGHTWADS: MANUFACTURING

HOW ARE THOSE INFORMATION SECURITY DOLLARS DIVIDED?



77%

AVERAGE RECOMMENDED INCREASE IN INFORMATION SECURITY BUDGETS IN 2003

36%

NUMBER OF COMPANIES THAT WILL ACTUALLY GET AN INCREASE

29%

AVERAGE EXPECTED BUDGET INCREASE OF THOSE 36% IN 2003

SOURCE: FROM A CIO MAGAZINE EXCLUSIVE SURVEY OF 276 EXECUTIVES. CIO IS A SISTER PUBLICATION TO CSO.



It's Not Easy Being Breached

**SURVIVING A SECURITY INCIDENT IS JUST THE BEGINNING.
THEN YOU NEED TO FIGURE OUT WHAT IT REALLY COST.**

BY SIMONE KAPLAN

A VETERAN CIO OF A NEW YORK CITY-BASED FINANCIAL SERVICES COMPANY LEARNED IN JULY 2002 THAT SEVERAL VITAL FILES HAD VANISHED FROM ONE OF HIS COMPANY'S 25 SERVERS. AN

employee had tried to find some information and failed. That's when IS discovered that there was, in fact, no company information on that particular server at all. Panicked, the CIO and his staff went into emergency mode. They soon discovered that a hacker had found his way through their firewall and wiped out all the production files on the server, leaving chaos and a couple of strangely labeled files in his wake. Two frantic days—and 15 hours of work—later, the alien files were deleted and the missing data restored through backup tapes. But it took an additional two weeks to be sure that the hacker hadn't accessed and tainted any of the company's 24 other servers.

All told, the CIO (who spoke on condition that his name not be used) reported that the breach cost the company \$50,000. But when asked how he came up with that number, he said he honestly couldn't say. Because he really wasn't sure.

"We didn't do a line-by-line breakdown of the costs because it didn't seem necessary at the time," he admits. "But consultant costs, loss of production time and overtime for the IT staff were part of it."

Even if CSOs can quantify the cost of a breach, few executives will talk on record about it. Companies have an incentive to downplay—or downright hide—such information. "It's embarrassing to admit that a hacker got through your firewall," says Tina LaCroix, CISO of Aon, an insurance provider. "Most companies won't give out the real information [about breaches]. They don't want you to know they have vulnerabilities because they make the CSO look bad."

"No one wants to be the company on the front page of *The New York Times*," says Thomas Varney, a director of technology assurance and security, who spoke on the condition that his Fortune 100 company not be named. But ignoring vulnerabilities won't make them go away. Every day (or so it seems), another consultancy reports dire new statistics on the cost of security failures. According to the 2002 computer crime and security survey from the Computer Security Institute and the FBI, 80 percent of the 503 security practitioners surveyed acknowledged financial losses due to security breaches, but only 44 percent were willing (or able) to quantify losses.

While circling the wagons is understandable, it's also counterproductive for the industry as a whole. "The bottom line is that CSOs are doing a pitiful job of tracking breach costs," says Michael Erbschloe, associate senior research analyst at Computer Economics, an IT investment consultancy. "They don't want to go public with the costs or even talk about it internally. The rationale is that, if CSOs don't know the numbers, no one else will

■ IN THIS STORY:

The reasons CSOs have trouble calculating the cost of a security breach and why it's important to try



“It’s embarrassing to admit that a hacker got through your firewall. Most companies don’t want you to know they have vulnerabilities because they make the CSO look bad.”

—TINA LACROIX, CISO OF AON



either, which cuts down on the likelihood that their company's reputation or stock price will take a hit." But he cautions, "CSOs need to wake up. Start sharing data, or we'll all be more vulnerable than we'd like."

"Every breach is different, and costs will vary from incident to incident. That's why it's incumbent upon the CSO to have an incident-response plan in place prior to a breach."

Creating a methodology for quantifying as many costs associated with a breach as possible is essential. Start by determining the value of your information and assets so that you can more easily find out what you lost. Break the incident down into every conceivable category because, inevitably, it has all been affected.

Hard costs—replacing servers or paying overtime—are easy to track. The real difficulty lies in quantifying nonattributable costs—the loss of customer trust or business. "Do more than simply calculate your physical losses," says Craig Goldberg, president of Internet Trading Technologies. "Look at what was lost in terms of customer, shareholder and employee information. What was the cost of lost business?" And don't forget the most serious damage—a blow to your company's reputation. "It's the gray areas that are usually the most significant in terms of cost but the hardest to prove," says Goldberg.

That's why cyberinsurance is a tough area, says Rich Mogull, research director at GartnerG2 Cross-Industry Research. Companies lack the solid actuarial formulas that enable them to figure out risks over time, so they underprotect—or overprotect—themselves (see "Safety at a Premium," Page 50).

KNOWING IS HALF THE BATTLE

It didn't take long for Ron Woerner, CISSP and information security officer for the Nebraska Department of Roads, to get a phone call from his ISP when an SQL Spida worm hit his department's systems in May. It found its way in via the Internet through an open SQL port that happened to have a blank administrator password, and then planted

several files to help it look for other targets through which it could spread.

"The ISP wanted to know why we were making so many SQL calls, so I got suspicious," Woerner recalls. "I asked him to block all our SQL calls to the Internet, since it's not a critical method of connection for us. Then I contacted our administrator for that particular system and confirmed that we were infected. At that point, I alerted our incident-response team, but I only put them on alert. The situation seemed under control, and we didn't want to go overboard with our response."

I updated our virus scanner on the infected system, found four files associated with the worm and removed them. We rebooted the server, did a sweep so everything was clean, and made sure our switch was configured to block the SQL port from our box to the Internet to prevent reinfection."

The whole incident took two hours to handle. Since it was a relatively minor attack and Woerner had a detailed incident-response plan in place, he was able to track the breach cost easily. The worm had infected an internal server, and during the downtime necessary to



A detailed incident-response plan helped Ron Woerner, information security officer for the Nebraska Department of Roads, track breach costs more easily.

Criteria for Determining the Cost of a Breach

- 1. System downtime.** What systems were out of commission and for how long?
- 2. People downtime.** Who was unable to work, and how long were they unproductive?
- 3. Hardware and software.** How much did it cost to replace servers, hard drives, software programs and so on?
- 4. Consulting fees.** If you needed extra firepower while fighting an attack or for a post-mortem analysis, how much did you spend on fees and other expenses?
- 5. Money.** How much were the salaries for people affected by the breach? Consider overtime pay or trades that couldn't be made during downtime.
- 6. Cost of information.** What was the value of information—employee, shareholder, customer—that was stolen or corrupted? How much did retrieving the information cost?
- 7. Cost of lost business.** Did clients take their business elsewhere? Were there opportunity costs—lost contracts or business deals—due to systems being compromised?
- 8. Incidentals.** How much did you spend on food, lodging and transportation for the people working to fight the breach? Were there additional facilities costs, such as power usage and electricity?
- 9. Legal costs.** What were potential and actual costs of litigating and investigating the incident?
- 10. Cost to your company's reputation.** Did you spend money on a PR campaign to control the damage? —S.K.

contain the infection, 15 employees were unable to do work on their computer. "Average pay for those workers was \$25 an hour; they were out for two hours, so I figure it cost about \$750," he says.

The incident's relatively small size doesn't diminish its importance as an example of why adding up the numbers can pay off in the end. Woerner took the \$750 number to his CIO and used it to demonstrate the need for a security budget and the necessity of taking preventive, instead of defensive, action. If the password on the SQL application had been

changed from the default or if the SQL port had been blocked, he points out, it would have taken only 10 minutes instead of 30 hours of work time away from the employees—and it would have cost nothing.

Because no data or system was seriously corrupted, Woerner had to consider only system and worker downtime, two of the most basic considerations when attempting to quantify the cost of a breach. But it can quickly get more complicated (see "Criteria for Determining the Cost of a Breach," this page).

Woerner says he could have padded the breach's cost to underline his argument to the CIO, "but if you inflate the cost, it will come back to bite you," he says.

LEGAL EAGLES

The industry's lack of a consistent model for calculating security losses often results in inaccurate loss estimates, "numbers that never would hold up in a court of law," says Varney, who spent years doing computer forensics with the Department of Defense and the Secret Service. "A company calls up and says, 'We've just been hacked. We've lost \$1 million.' They pull a number out of the air," he says. "I ask how they got that number, and it turns out they're just guessing."

Varney says many CSOs don't realize loss estimates are not enough to prosecute security offenders. "If the amount varies from what the prosecution presents, the defense will poke holes all over your case," he says.

Law enforcement has minimum monetary damage requirements for prosecuting a security case. The amount depends on the jurisdiction, Varney says, but it can range from \$500 to \$500,000. The numbers must be carefully catalogued, and prosecutors must be able to prove them. Otherwise, a lawsuit might not go the way you think it should.

Case in point: In September 2001, a jury found Herbert Pierre-Louis guilty under the Computer Fraud and Abuse Act for launching a virus attack on four offices of Purity Wholesale Grocers in 1998. According to Purity, the virus shut down operations for a week and caused at least \$75,000 in damage, well over the \$5,000 minimum. But in April, a federal judge threw out the conviction because the jury ruled that the virus didn't cause enough damage to rate as a federal crime. The breach

occurred before the Act was amended in 2001 to cover lost revenue from suspended operations and repair costs from interrupted service, and thus the damages as defined by the law did *not* total \$5,000. Pierre-Louis's conviction was nullified.

Trying to nail a hacker is just the beginning. The concept of downstream liability is also a concern, says Aon's LaCroix. These days, viruses jump from company to company. If a company is deemed negligent in deploying adequate security, there's a potential for third-party lawsuits from others affected afterward. "You are no longer responsible for just your own security," LaCroix says.

Ask Ziff Davis Media. Deficient security and privacy protections cost the publishing company at least \$125,000 in August 2002 when an online subscription promotion exposed subscriber information, including credit card data, to public view. Several subscribers subsequently became the victims of identity theft. In a settlement with the New York state attorney general, Ziff Davis agreed to pay a total of \$100,000 to three state governments, as well as \$25,000 in compensation to 50 customers whose credit card data was bared during the incident. If all 12,000 subscribers whose information was revealed had provided credit card data to the company, the settlement could have reached \$18 million, according to John Pescatore, an analyst with Gartner Research.

Until someone comes up with a way to prevent breaches from happening at all—and, as we've pointed out in this issue, risk will never be reduced to zero (see "The Art of Uncertainty," Page 44)—CSOs will have to deal with the aftermath of incidents and trying to come up with a cost for the whole shebang.

"We learned one lesson really well," says the anonymous CIO of the New York financial services firm. "Understanding what you're spending on security cannot be overrated." ■

Staff Writer Simone Kaplan can be reached via e-mail at skaplan@cxo.com.

For more on security breaches and what to do when they happen at your company, visit CSOonline.com's **THREATS & RECOVERY RESEARCH CENTER**. Find it on the Web at www.csoonline.com/threats.



The Art of Uncertainty

TO HEAR FRANK BERNHARD TELL IT, ECONOMICS IS ANYTHING BUT THE DISMAL SCIENCE—AND RISK MANAGEMENT IS THE KEY TO A CSO'S SUCCESS

THE ECONOMICS OF RISK. IF YOU SHUDDERED WHEN YOU READ THAT, THEN YOU'RE LIKE MOST OF US WHO SEE IN THE PHRASE A MIGRAINE WAITING TO HAPPEN. PROBABILITY CURVES, CONTRAPOSITIVES,

null hypotheses and egghead professors with Nobel prizes. The economics of risk is not for the faint of heart.

Economist Frank J. Bernhard must have a strong ticker, then, because he'll talk to you all day (trust us, he visited our office) about the economics of risk and—with eagerness, verve and a Magic Marker to jot down some Greek letters—expound on behavioral economic theory. Bernhard is a technology economist and managing principal with Omni Consulting Group in Davis, Calif. His latest book, *Beyond Collaboration: How Supply Chains Meet Demand Chains* (CRC Press, 2002), describes economic evidence of the sustainable partnerships and innovation that will unfold in the next century.

Thankfully, Bernhard's greatest skill seems to be his ability to wax statistic but then translate it into a language that *you* understand—and can use: Security insurance is like Goldilocks. Car thieves know how much

you should spend on security. He even condones (gasp!) guesstimation as a risk management tool.

Managing Editor Elaine M. Cummings spoke with Bernhard to learn what in the world an economist thinks of the current state of security, how CSOs should be thinking about the economics of risk, and, most important, how they should be communicating it. Read on to see what Bernhard had to say. We promise you won't shudder once.

CSO: The concept of risk can be a little nebulous. Is there a working definition?

Frank Bernhard: Yes. Simply put, risk is something that happens if you don't do something else—more specifically, it's a computed chance or probability of something *negative* happening.

Are economic risk and business risk the same things?

No. Economic risk can involve things like supply-and-demand conditions or geopolitical events. Business risk extends to the outcome of not getting investors. Or losing customers. Or the failure of a product or service. Business and economic risk can coexist in

various cycles of the economy and may be interrelated to other causal relationships, such as waning demand coupled with diminished investor confidence.

■ **IN THIS STORY:** Find the threshold for how much risk to accept ■ Learn to set priorities like an economist



**“Whenever you look
at security, whether
you’re a CSO or an
economist, you have to
look at it as a trade-off.
You need to ask, Am I
trading something of
positive value that’s
going to help me be
more productive, or will
it cost me productivity?”**

**—FRANK BERNHARD,
TECHNOLOGY ECONOMIST
AND MANAGING PRINCIPAL,
OMNI CONSULTING GROUP**

Why does an economist care about risk?

Economics is about choice, about how we allocate resources. It's about trading one resource for another. So as an economist, I focus on the outcomes of risk, which I see as a binary situation—that is, something either happens or it doesn't. One resource has to be conserved or maximized to influence an outcome—that guides some of the primary influencers in making an event happen or not. And I'm interested in the things that contribute positively to the risk equation. I could get fancy and tell you that the null hypothesis of something happening is contrapositive to one outcome over the other....

OK, stop there. So should a CSO look at risk like a businessperson or an economist?

Well, both are interested in the mitigation of risk. But whenever you look at security, whether you're a CSO or an economist, you have to look at it as a trade-off. You need to ask, Am I actually trading something of positive value that's going to help me be more productive, or will it cost me productivity? If you stop and think about the real effect of security, in addition to perhaps mitigating risk, you've probably slowed things down. Everything in the enterprise is scarce in resources and abundant in demands. The challenge is to achieve balance between sensible investment in security and not lose productive business ground in the process.

When it comes to security, most people talk about the technology of security, not the economics of it.

That's because risk is difficult to measure. And when something is difficult to decipher, we tend to look at well-defined solutions of technology instead of focusing on its risk-reduction perspective.

So that means you can measure risk?

Risk is certainly measurable. Since risk is a factor of probability and it has an outcome, you can measure it and model it and start to understand its core attributes with some level of specificity. And then you can develop some sort of rubric or schedule as far as how to curb risk or induce risk. Like a simple scorecard that takes inventory of risk types and assigns the cost of such outcomes, a

CSO can begin to apply sensitivity analyses to derive a calculated picture of an enterprise's given risk model.

But how can you anticipate every risk? If you look at homeland security, for instance, most of us never imagined before 9/11 that some of those things could happen.

Sure. The new risks we're dealing with today simply have to be added to the inventory of risk. It's a pool of risk-based scenarios. Sadly, it's becoming something more than just the benign and basic risk elements. Security officers today need to take inventory of their risk elements in their environment and their IT landscapes. And then they need to start by assigning some sort of probability—or at least some ranking measures and triage—to the risk equation.

Where do you begin?

Take an inventory of all the different possible risks—like the loss of data—and then assign probabilities to those risks. The number of risks can extend to infinitum, but you can start by deductively measuring the most prominent, rather than the highly obscure.

When do you know the optimal timing to take risks, when to be risk averse?

I think that it's human nature to be risk averse. Some people have less appetite or propensity for risk. But we are, at our core, risk-averse people. That means we want to challenge the notion that something we don't want to happen, in fact, will. So we have to ask, If I do X procedure or make Y decision, then is Z outcome going to occur? And have I set thresholds for myself?

What kind of thresholds?

Life is never without risk. Every day we go out into the world, drive our cars, get on airplanes, get on the Internet. And we have a certain amount of risk that we accept in doing those things. In economic terms, we can't mitigate risk to a zero value—there's no such thing as zero in risk. It's all about how much risk you're willing to take on and actually absorb. So you set logical thresholds for what you're willing to accept as an appetite for risk. In the stock market, for instance, investment performance is calculated by



assigning what we call a risk coefficient. You can actually put numbers to the predicted risk performance. If the risk coefficient is computed to be less than a market-equilibrated threshold, then your investment position is said to be conservative. If the risk coefficient is greater than that threshold, you're said to be risk dominant. In other words, you're willing to accept some measure of risk as a higher economic payment in the event of a positive outcome.

Likewise, you have to set thresholds in your enterprise within your control for the amount of risk you're willing to accept. Then determine where to establish a coefficient that's within your comfort zone.

How do you determine that threshold?

First, consider your resources and possible contingencies. If the risk of losing a server is greater than the ability to recover the data in that server, then do not proceed with whatever procedure might jeopardize the loss of the server. You start with asking yourself what the very essence of risk is in your enterprise. The answer will be very individualistic. And the trade-offs are numerous.



"There's no such thing as zero in risk. It's all about how much risk you're willing to take on and actually absorb."

—FRANK BERNHARD

What would you identify as the number-one area for information security concern today?

It's threefold, really. First, you need to control access. Most attacks happen because people have access to systems—not the server, per se, because the server is the only end point of access. Access happens when I walk into the building. So you need to think about access cards that give free-moving entrance to facilities. Access may also be logging on to a network. So you create passwords or authentication to the network.

The second part is to think about information assets and their hierarchy in the organization. For example, is your customer data the most important asset to running your organization? Or is it the financial systems? The supply chain system? Or your data warehouse? And do your employees use the data on their desktop, or is it used strictly on a protected server? You have to start by doing some hierarchical mapping of what your information assets are to prioritize what is most at risk.

Then, thirdly, you need to consider mobility—the combination of access and assets. I mean, how do people interface with

your systems? You have wireless LANs [local area networks] and VPNs [virtual private networks], and all that comes with technology, but the problem is, you still have people in the equation. And people are using systems and assets outside of the wired environment that they've traditionally operated in. So they have to come back to the basics of how to control that mobility.

And then how do you know how much to spend—and on what—to mitigate risk?

It's difficult to know how much spending is enough. You need to determine how much risk you're willing to accept and assume. And then financially and methodically compute that risk. And that's where most people really get stuck. Either the tendency has been to spend without concern for a bottom-line impact or go overboard with governance that maniacally destroys the productivity of an organization.

Guesstimation is not an exact science, but it's a good start. Pay attention to that visceral feeling about where you think your risk is most obvious. Then boil it down to the top three areas driving security: access, information assets and mobility. That makes up about 85 percent of your concerns.

And the other 15 percent?

Is around the physical buildings, facilities and perimeter security—largely those elements of risk being waged against in the efforts of homeland security. If you think about security in general, the safety of a democratic and civil society imposes enough moral restraint to diminish rampant chaos. But security does extend to physical infrastructure of organizations and the challenge to maintain order amidst the outbreak of terrorism and overt violation of public law.

Spending on insurance is just one way to mitigate risk. How much is enough there?

It's a tale right out of *Goldilocks*. Typically, people sign up for either too much or too little insurance. They don't ever have just the right amount of insurance. You have to start by asking, What's the valuation of the assets I'm protecting? What's the probability of risk assignment? And then what's the cost to protect those assets?

To spend the appropriate amount on insurance, you want the cost of insuring an asset to be less than or equal to the cost of the asset itself. The premium must justify the means of loss protection. Pooled risk dictates that some loss is inevitable but the premium schedule for such assurance should be commensurate with the risk basis. So if an insurance policy protects your million-dollar asset and the policy costs \$900,000—and the risk of destruction or complete loss is, say, 15 percent—then the risk of loss is grossly disproportionate to the premium paid for asset assurance.

The numbers may be high as an example, but they speak to a point. Insurers want the least of risk for the maximum amount of premium. The enterprise wants the maximum amount of protection for the least amount of investment. Therein lies the economic argument for investment and risk mitigation: The equation must balance at a level of security adequacy and fiscal prudence.

Think about buying an extended warranty on a television, for example, where the asset life is relatively short but the policy is almost 30 percent of the item's original cost. If you divide the useful life by its original cost and compare the premium for replacement, the math seldom favors the consumer. Much in the same way, companies spend on protecting their assets, but they can actually get to a point of diminishing returns.

How do you optimize that spending on security?

First, it comes down to common sense. You want to be risk cautious, but you don't want to be risk absurd. The practical question you have to ask is, Does the behavior or the policy in the governance of my enterprise match the level of risk that it's willing to accept?

But it also comes down to what we label the economic value proposition. You have to weigh the economic value being created by security before you invest in it. And I come back to this point of diminishing returns. Does doing all of this—going to the airport and having to show your ID five different times to get on board the airplane—effectively mitigate the risk of an unknown passenger gaining access to get on that plane? What if the identity is forged? It seems you may have done nothing more than cause



longer lines. You've certainly slowed productivity, and you've prevented people from doing the job they set out to do. Most security measures in some way or another harm the economic productivity of an organization or a customer base.

But how do you spend just enough to protect yourself against the negative outcome of something that you're trying to protect against?

Therein lies the ultimate economic equation. You only need to win the race by a nose. Basically you're trying to optimize the formula to say that if you put X dollars into security, you have Y risk that you feel comfortable with. And the investment sign should always be less than or equal to the amount of risk that's being borne.

What do you tell the CEO who asks, So why should I buy security?

Because you gotta have it. It's like, how do you sell the value of a dishwasher to a restaurant? You've got to have it because you've got to have clean dishes. Think of it not as an ROI problem but as an economic value discussion. What economic value does that dishwasher drive? Maybe it's a substitute for manual labor. We have to start with the conclusion that we want to have clean dishes. If you don't, that's a health-code violation.

I don't think people have a hard time understanding that security is something we have to offer because, if we don't, we're open to liability. That's a secondary outcome. And if we're open to liability, we may get sued. So we want to do those things that are obvious within man's control. That's the litmus test—that it's within a reasonable person's control to mitigate risk and ensure that they're not liable. They don't want to act with negligence, the way a restaurant doesn't want to have dirty dishes. It's a quality-of-life issue. If you don't have security, what happens when that worm annihilates your database? Then you've got a real problem.

How do you sell that idea to a CEO?

The CEO sits atop the jungle and looks at the landscape and says, Here's where we're going as an organization, and here are the

The Top Five Concerns for a CSO

1. ACCESS

Control to the enterprise and basic functions of the enterprise should be high on your list.

2. ASSETS

Consider information as well as operations. Protecting them is your *raison d'être*.

3. EMPLOYEE MOBILITY

Think about how assets can be moved around.

4. HUMAN CAPITAL

Pay attention to the telltale signs that could predict an employee threat.

5. PERCEPTION

You need to make employees feel safe without going overboard. Knee-jerk reactions won't gain any ground or achieve a competent effect.

risks that we're willing to absorb and thwart with appropriate security. The budget is almost formulaic to the extent that companies look at their annual revenue, productivity, assets that drive productivity within them, and they have to compute a value. Maybe it's a small percentage of their total revenue that they apply to security. It's almost like their marketing equation. How much do you spend on marketing? It's a percentage of sales. Some companies don't want to spend anything on marketing. Others spend in the double digits. What results are you trying to achieve and, in this case, what risks are you willing to mitigate, to bring it back to a cost basis? But no matter what, the CEO has to buy into the strategy. Think of the former U.S.S.R. and the Russian spending race in the 1980s to build a superior military presence, but a strategy that ultimately caused the demise of a bankrupt nation's inability to take care of its people—on the homeland. Your competitors might invest in Star Wars as a

defense strategy, but don't always mimic their behavior to secure your future.

How do you measure the economic value being created by risk?

Every time you have a restriction there's a consequence. And it's an economic consequence. We talked about standing in line at the airports. What does that mean? It's about business productivity. And when it's hampered, it really doesn't do you a lot of good, especially when you're in a recession.

There is no substitution for common sense. There is a rational human mind that wishes to counteract the devious human mind, and that's what you're dealing with when you think about risk. Not everything that happens as far as risk is human driven. You can have the risk of losing your data because the store server collapsed. If the mail server suffers a blow to its caching drive—basically that's a risk, right? How do we protect against that? Well, there's tape backup or there's a failover situation so that the system keeps working. So we want to look at risk in terms of probability assignment; you couple that to rational human thinking and common sense, and look what you get. You get something that's much greater than anything you can put together in a mathematical sense.

So, if a structural balance between spending and just enough security is the goal in mind, then how effective is the whole mix?

Let me answer this way: Travelers are reassured that flying aboard commercial aircraft is safe, but that's not exactly true. In reality, safety in flying is about managing risk. Likewise, security is about managing risk. While total protection from loss can never be achieved, we act with discretion toward spending appropriately to protect those assets at stake. ■

How do you assess risk? E-mail Managing Editor Elaine M. Cummings at cummings@cxo.com.

For more on **MANAGING AND ASSESSING RISK**, visit CSOonline.com's Strategy & Management Research Center. Go to www.csoonline.com/strategy.

CSO Perspectives™

Today's security executives meet at the

CSO Perspectives Conference

As an executive responsible for securing and protecting an organization's information assets and infrastructure, you are constantly searching for how to better define your mission and responsibilities within the enterprise. You need a forum in which you can address your own unique set of business-level challenges—and network with your peers.

June 17-19, 2003
Hotel del Coronado
Coronado, California

CSO Perspectives meets those needs

with an educational and networking conference just for you—chief security officers (CSOs) and senior technology decision-makers (CIOs). At CSO Perspectives, you'll gain firsthand knowledge from industry experts and your peers that can enhance your organization's security strategy.

You'll have the opportunity to:

- Exchange best practices in balancing risk and responsibility
- Learn from your peers what works in the real world
- Explore creating a culture of security
- Understand the current thinking on key issues and trends
- Uncover the hidden threats of legal liability
- Examine emerging technologies that will impact your enterprise

Visit us at **www.csoperspectives.com**
or call 800 366-0246.



The Resource for
Security Executives



Safety at a Premium

ARE YOUR INTANGIBLE ASSETS PROTECTED? HERE'S HOW TO CHOOSE THE
RIGHT INSURANCE POLICY FOR YOUR COMPANY. BY DAINTRY DUFFY

IT CAN GO BY ANY NUMBER OF NAMES—THE CYBERHURRICANE OR THE DIGITAL EARTHQUAKE—BUT THE CONCEPT IS THE SAME: IT'S ALL ABOUT COMPUTER CRIME. CRIME AT A MAGNITUDE SO enormous that it threatens to disrupt the Internet, affecting the communications and business operations of a large number of companies simultaneously.

A constant onslaught of minievents have primed CSOs for the credibility of this notion. From the I Love You virus to Nimda, Code Red, Klez and Bugbear, security executives have had a sufficient taste of the financial costs and management headaches associated with fending off cyberattacks to understand that the threat to their companies is real. And potentially greater hazards loom on the horizon—superworms and cyberterrorism to name just a few.

So call it what you will, CSOs increasingly stand poised for The Big One.

While such an event poses an ever-present fear for CSOs, insurance companies see it as both a business opportunity and a challenge. Many insurers are marketing e-risk insurance products specially tailored to address the corporate security risks posed by the Internet, but the process behind offering e-risk insurance is currently much more an art than it is a science.

CYBERCOVERAGE

Mainstream business insurance policies were never meant to cover the astronomical financial and reputational costs that a virus or other technology-related business disruption can cause. The publicized theft of sensitive corporate data like credit card numbers has hastened a number of companies, such as Flooz.com, into bankruptcy. And in just the first five days of circulation, the I Love You virus cost businesses \$6.7 billion, according to researcher Computer Economics. The insurance industry's reaction to the growing risks posed by Internet activity has been twofold: First, they've written exclusions into their basic business policies that Internet-related risks will not be covered. Second, they've seized the opportunity to develop and market specially tailored cyberinsurance or e-risk policies that offer specific coverage against hackers, viruses and cyberextortion. Policies like that would once have only made sense for customers that were betting their entire business on the Web, but the Internet has become so tightly woven into the operations of most large organizations that that is no longer the case. "Most companies with websites have gone from putting out brochures to being high-intensity publishers," says David O'Neill, vice president for e-business solutions at Zurich North America. "That opens the door to copyright, trademark infringement, electronic extortion and other computer crimes."

Policies vary widely in terms of what they cover. Some take a cafeteria approach, allowing companies to pick and choose only

■ IN THIS STORY:

Determine how much insurance you have and how much insurance you'll need





the specific coverage they require. But the challenge is that, while there's no shortage of security statistics coming out of law enforcement and security research companies, very little has been done to map those figures to the financial losses actually incurred by companies. Consequently, insurers are still deciding how to price the coverage. And because the actuarial models behind the policies are vague and differ greatly between insurers, companies looking for an e-risk policy are often comparing apples with oranges. To further muddy the waters, the pressure on companies to assess, mitigate or transfer any perceived risks to their business viability has never been greater. So what's the risk-sensitive CSO to do? Here's what you'll need to know when evaluating cyberinsurance.

PUSH AND PULL

Many corporate risk managers assume their company's commercial property/casualty policies will cover any business disruptions that result from security breaches. They're often wrong. In a recent survey of financial institutions mentioned in *NYSE Magazine*, more than three-quarters of the 76 percent of respondents who identified e-commerce as their number-one risk-management issue also erroneously stated that they were covered for cybercrimes under their traditional insurance policies.

Most standard business insurance policies cover only the damage or theft of tangible assets like buildings or equipment. "Computer code is deemed to be intangible," says O'Neill.

"Property and casualty policies were never written to assess these exposures and were never priced to include them."

Until recently, traditional property insurance may have provided some coverage for virus-related exposures, but as of January 2002, the majority of insurers eliminated it as well. The reason: the reinsurance or secondary market—which functions like a bookie with whom the primary insurance industry lays off its bets to minimize undue risk concentration—is concerned by the notion of the cyberhurricane. "It could affect thousands of companies simultaneously with no geographic locus," potentially causing too much exposure to individual insurance companies, says Jeffrey Grange, senior vice president and global manager of fidelity and professional liability products for The Chubb Group.

The second reason insurance companies are moving cautiously in that area is the reality of insuring a post-Sept. 11 world. The prospect of significant business disruption to the telecommunications network on which technology platforms run is that much more real after 9/11. It is also considered likely that a next wave of terrorist attacks could come in the form of cyberattacks aimed at disrupting significant portions of the critical infrastructure and targeting the technology backbone of various enterprises.

The result of those market pressures has been a retrenchment on the part of insurers and reinsurers that—after paying out tens of billions of dollars in 9/11 losses—have lost

their appetite, at least in the short term, for a new market in which so many uncertainties exist. While industry insiders such as Grange expect that to be a temporary market dynamic, the consequence for companies currently seeking cyberrisk coverage will be that premiums will be higher and the policies that already require a fairly stringent security audit will be harder to qualify for.

Similar economic pressures are making cyberinsurance that much more important for companies whose risk-management practices are facing growing scrutiny by government groups and investors. For many companies—particularly those in technology, financial services and pharmaceuticals—their most valuable corporate assets are in the form of data. The Financial Accounting Standards Board (FASB) is now directing companies to state the value of those intangible assets in order to more accurately quantify the business's market value. As more companies discover how large a percentage of their market capitalization is in the form of computer code and stored data, the pressure to properly protect it with high security standards—and thereby transfer through insurance the risk of loss—is growing.

Regulatory developments are also going to increase the pressure on companies to account for and mitigate risk. The Basel Capital Accord, which was developed in 1988 by an international banking organization to promote the safety of the global financial system, has been updated with new regulations that are due to take effect in 2004. The new accord will specify methodologies by which financial institutions must measure their operational risk—the risk of direct or indirect loss due to inadequate or failed internal processes, people and systems or external events. That risk measure forms the basis for a calculation of the amount of capital an institution must set aside in reserves to cover potential losses. For the banking industry, many of those operational risks will revolve around the use of technology, and being able to offset some of that risk to insurance will be an attractive option and may reduce the amount of capital that an institution has to keep on hand.

WEIRD SCIENCE

Quantifying the losses from a breach in secu-

Most cyberinsurance policies cover some or all of the following areas

Internal criminal acts. Coverage for malicious acts perpetrated by employees using computers.

Hackers. Losses resulting from a direct attack on your company's network, or the use of your network as a platform or gateway to launch a third-party attack.

Viruses. Coverage for the costs associated with a virus-related interruption in business and the reconstruction of any lost data.

Media liability. Coverage for exposures related to the misuses of trademarks, domain names, plagiarism, copyright infringement, defamation and libel on the Internet.

Privacy violations. Coverage for exposures stemming from the misuse of personal information.

Crisis management. Funding provided to help a company handle the public relations fallout from a security breach.

Global risks. Coverage provided for security threats regardless of where an attack is launched from or the damage that occurs.

Here's what to ask your insurance company when shopping for a cyberinsurance policy

COVERAGE

- Will you perform a gap analysis on my company's current business insurance policies to determine where there may be holes in coverage?
- What types of e-risk events do you cover and which do you exclude?
- Do you offer coverage for cyberlosses resulting from terrorism?
- Are additional costs for crisis management and communications included in the policy?
- What is your coverage capacity? (Should be \$25 million at minimum.)

THIRD-PARTY PROVIDERS

- Whom do you partner with for risk assessments?
- Can we choose from a group or is there only one option?

EXPERIENCE

- How long have you been covering cyberrisk?
- How many policies have you issued?
- Will you provide a client reference?
- How familiar are you with my industry and business?
- Do you have the in-house staff (underwriters, claims specialists, legal professionals and technologists) to handle the claims process?

INTERNATIONAL COVERAGE

- Does the policy have a geographic definition? If we are sued abroad will the policy cover any liabilities?
- Does the company have its own global operations or does it partner with another carrier?

ity is a complex process—and one with which the insurance industry has struggled for years. After all, if somebody steals the computer on your desk, that's pretty much a known value and the claim is for the cost of replacement.

When data is lost, the value is much harder to quantify. One could calculate the cost of reconstructing that particular record, but that figure doesn't account for the intellectual property value the stored data can have.

And what if the data were a pharmaceutical formula for a groundbreaking new drug and it was stolen and sold to a competitor? The entire company is less valuable because that information has been compromised. "The value of data is difficult to determine, and the value is often only relevant to that particular organization," says Doug McCarthy, senior operations analyst in technology underwriting for The St. Paul Cos. Given the difficulty of placing a value on that kind of intangible information, it's important that CSOs work with an insurer that shows a keen understanding of its industry.

Most lines of coverage in the insurance industry are backed by precise actuarial tables that inform the pricing process. For example, an auto insurer can look at the accident and theft rates for the state you live in, your driving record and the value of your car, and figure out precisely how much it should charge for coverage. The actuarial tables for cyberinsurance are still a work in progress, but an interesting partnership has been developing between the government and the insurance industry to try and flesh out those figures.

The Critical Infrastructure Protection Board (CIPB), which was established by President Bush in October 2001, has taken a keen interest in the insurance industry. When a weather-related disaster occurs, the government can send in the Federal Emergency Management Agency, or FEMA, to provide recovery assistance and funding, but there is no such mechanism for a cyber-based event. With nearly 90 percent of the critical infrastructure in the hands of private industry, the government wants to ensure that there is a relief function in place. The government is hoping cyberinsurance will gain currency among companies and assume that role. To make that happen, the CIPB has developed a working group with insurance industry members to try to pool the data that exists within the government and the insurance industry to develop actuarial tables. It's a difficult process that's expected to continue into 2005. "The data exists in many sources within the pri-

securiQ

Beyond Anti-virus Protection – securiQ

For all your e-mail security challenges

- content filtering
- image scanning
- spam blocking
- archiving
- enhanced virus protection
- encryption
- legal liability

Protect Your Messaging Platform Today.

Be Prepared for Tomorrow.

securiQ – Maximum E-mail Security.

Call Toll Free – 877 – GROUP – 55
www.group-software.com

 **GROUP
TECHNOLOGIES**
Intelligence for e-mail

vate and government sectors,” says Grange, a member of the working group. “There’s a complete alignment in interest between private sector insurance and the government in terms of cyber-risk management and the need to understand the bottom-line costs.”

While sharing data might sound like a fairly simple process, it’s fraught with complexities: from the age-old problem of companies unwilling to confess the details of a security breach to the absence of legal precedent for the liability that companies could face in a court of law due to a security breach. “Nobody really knows what data they’re looking for,”

“The best time to insure a company is *after* the fire,” says O’Neill. “That’s when they’re likely to have the best fire suppression system and sprinklers.”

The second area that insurers are looking at is the fundamentals of your business—the size, revenue base, industry and management. In the current economic climate, it’s worth noting that financial health is also a determining characteristic. “Financials are a good indicator of being able to safeguard your company,” says O’Neill. “Less-than-stellar financials suggests that you don’t have the capital to put into your electronic platform.” All of that

his company’s needs. And forging a close relationship with the company’s risk manager will be critical to that process. “Often, it’s the first time they’ve even met one another, which is frightening,” says Tracey Vispoli, assistant vice president and cyber solutions manager at The Chubb Group. “We’re there to talk about risk, not technology. How much risk the organization wants to keep and how much it wants to transfer. When you put it on the business level of risk, everyone speaks the same language.”

Here are some other things you can do.

Prioritize assets. Working together, the CSO and risk managers should develop an

“The best time to insure a company is after the fire. That’s when they’re likely to have the best sprinklers.”

—DAVID O’NEILL, VP FOR E-BUSINESS SOLUTIONS, ZURICH NORTH AMERICA

says a source close to Richard Clarke, President Bush’s cybersecurity adviser. “Companies have traditionally not factored in cyberlosses. When Code Red and Nimda happened, some companies took a big hit, but there were no metrics for tracking what it cost—lost productivity, the IT department’s time. Nobody knows how to estimate it.”

Given that, insurers are taking two basic elements into account in setting the premiums for their e-risk policies. The first is the security audit that most insurers require as a prerequisite to coverage. The audit (conducted by a third-party security management company) usually involves the submission of an application overview of the company’s operations and completion of a security questionnaire. Most auditors will also take a close look at the security policies a company has in place—how often passwords are changed and antivirus updates are run, and the policies that govern employee access and use of systems. Depending on the policy’s requirements, that step may be followed up with penetration testing and social engineering exercises designed to plumb the company’s susceptibility to external attacks. And in case you’re thinking that the serious security breach you had this year will make you an unattractive candidate to an insurer, you shouldn’t worry.

information becomes part of the underwriting process and, like a home inspection, the insurer and applicant will often negotiate about certain areas that need to be fixed in order to strike a deal. Once an applicant meets the qualifying level of security, it can go further and implement additional security measures that the audit recommends. And their premium will lower accordingly.

The process behind the pricing of the embryonic market for cyberinsurance is not all that different from the way other markets have developed. “I compare it with the way the environmental market built out,” says Harrison Oellrich, a managing director of Guy Carpenter & Co. “The initial forms and exposures were very similar in that there was no data to underpin the rates. People began by putting a very restrictive policy form with very high pricing on the market; and over time, as they began to develop experience, they were able to broaden policy forms and modify the pricing significantly.”

TIPS FOR THE CSO

Given the uncertainty surrounding the pricing of cyberinsurance and the growing pressure on companies to seek such protection, the best thing a CSO can do is to judiciously examine each policy to determine how well it matches

inventory of the company’s technology risks and assets, prioritizing the assets that need to be recovered first and the points of failure that could result in widespread risk to the organization. “While CSOs tend to be experts in risk identification and mitigation, they have little experience with the alternatives for transferring the financial impact of losses from the balance sheet—in other words, how can they hedge their bets,” says Grange. “That’s why a risk management model applies.”

Assess weaknesses. A thorough risk analysis should include a gap analysis. What is the company’s current security-breach coverage under other policies? Pay attention to the gaps between physical and cybersecurity coverage. Most traditional insurance policies will cover physical security breaches within the four-wall operations of the company—like the theft of a computer from someone’s desk or a break-in where an individual absconds with sheafs of valuable information. But the physical and cybersecurity worlds intersect in so many different ways that a thorough gap analysis should be done to uncover any potential holes in coverage. One technique for accomplishing that is to purchase cyberinsurance coverage from the same insurer that provides your traditional physical coverage.

Share information. CSOs should also open

a dialogue with other business leaders to ensure that they understand what cyberinsurance does—and does not—cover. The scope of most policies is quite narrow, and while it may underwrite failures in the company's e-commerce operations or applications, it won't underwrite the Web, for instance. And if the ISP goes down and the company can't conduct business, it's likely the loss won't be covered. All the important players in the corporate hierarchy should understand the policy's boundaries so that when there is a security- or technology-related problem, everyone has the same expectations.

Business unit leaders can also help CSOs hammer out the right policy with insurers. For example, if a business unit conducts \$150,000 over its e-business network per hour, it will be important to ensure that the policy indemnifies the system in question for at least that amount.

Pay attention to detail. CSOs should note any exclusions that are written into an e-risk

policy. Some insurers will offer coverage for security breaches that are perpetrated by external individuals, but not by employees. The assumption is that an internal user poses a far greater risk and can inflict substantially greater losses. Some companies in the past year have also inserted exclusions into their policies that stipulate they will not cover cyberlosses as the result of terrorism. Determining whether a hack is an act of terror could be a sticky issue between CSOs and insurers. At The Chubb Group, Grange notes that they have decided not to make a terrorism exclusion. "It seems to us that, from a customer perspective, one does not make a distinction between a regular hacker and a political hacker," he says. "I don't care who launches the virus against you, a virus is a virus is a virus. Just like a fire is a fire is a fire." Some companies that have a terrorism exclusion will offer you the opportunity to buy that coverage back if you wish.

Know the facts. One final—and perennially difficult—issue is if, when or how the authorities will be notified in the event of a breach. O'Neill suggests that CSOs have that conversation with their insurer up front as some companies have policies that mandate calling the authorities, which can sometimes make it harder for the company to get back up and running. "When you engage the feds, they will draw yellow tape around the affected systems and impair a company's ability to gain forensic information," says Sanjay Mehta, vice president of business development at Tru-Secure. If the systems are physically quarantined, the effort to restore business continuity can be dragged out indefinitely.

The best advice for CSOs that are weighing cyberinsurance coverage is the familiar adage: Let the buyer beware. Many of the differences between individual cyberinsurance policies are found in the small print, and CSOs who carefully analyze the details of their coverage will be better protected if—or when—The Big One comes along. ■

E-mail Senior Editor Daintry Duffy at dduffy@cxo.com.

Know your company's e-risks? Read about the vulnerability scanning and assessment markets in **TESTING FROM THE INSIDE OUT**. Go to www.csosonline.com/printlinks.

For more information on e-risk coverage, check out the following sites

American International Group
www.aig.com

The Chubb Group of Insurance Cos.
www.chubb.com

Lloyd's of London
www.lloydsolondon.com

Marsh & McLennan Cos.
www.marshmac.com

The St. Paul Cos.
www.stpaul.com

Zurich North America
www.zurichna.com

iQ Suite

Beyond E-mail Security – iQ.Suite

35 billion e-mails will be sent daily by 2005*.

Get ready with iQ.Suite for all your e-mail and business process security, organization, and management.

Protect Your Messaging Platform Today.

Be Prepared for Tomorrow.

iQ.Suite – Maximum E-mail Security, Organization and Management.

* Source: International Data Corporation

Call Toll Free – 877 – GROUP – 55
www.group-software.com

 **GROUP TECHNOLOGIES**
Intelligence for e-mail

CIO Magazine's Eleventh Annual

Enterprise Value Retreat & Awards® Ceremony 2003

JANUARY 26 – 28, 2003

MARRIOTT DESERT SPRINGS

PALM DESERT, CA

Meet—and learn from—this year's award winners

Only a few organizations make the grade each year. *CIO Magazine's* Enterprise Value Awards are the most prestigious in the IT industry. Each winning company shares the good, the bad—and the just plain ugly—on how they built an award-winning system, and what value it brought to its users and to the enterprise.

New Format! New Agenda! New Moderator!



PETER WEILL
*Director, Center for
Information Systems
Research, MIT Sloan
School of Management*

Roll up your sleeves with an all-new business/IT case study:

Meet in small groups to discuss the case in-depth, and present your findings and recommendations.

Explore new ideas from thought- provoking speakers:

We'll bring you speakers who make you think beyond the boundaries of your day-to-day challenges.

Relax with your peers:

Network at the *CIO* Golf Tournament and Super Bowl XXXVII Party

Put it on your calendar now!

Call us at 800 355-0246 or visit
www.cio.com/conferences.



The Magazine for Information Executives

machine

Technologies, Tools
and Tactics
Edited by Derek Slater

shop



Next Year's Hot Security Tools

Today's pain points are tomorrow's vendor opportunities By Simson Garfinkel

IF YOU WANT TO PREDICT THE most important information security tools for CSOs in the coming year, just look at the problems that CIOs are trying to resolve today. Whereas today's security tools are intrusive, clunky and require significant commitment from both staff and users alike, tomorrow's tools will increasingly be automatic and even autonomous. Whereas today's tools are focused on delivering technical capabilities, tomorrow's tools will be focused on delivering concrete results. Finally, as

CIOs and executive management focus on what ails them, more and more classic IT problems are going to be rephrased—right or wrong—as security problems.

That's sure to open the door to new solutions. Unfortunately, it will also open the door to new disappointments, as immature tools are frequently not a good match for the problems they seek to solve. So along with next year's likely winners, I've noted some widely hyped technology areas where available tools still earn a "needs improvement"

grade. (Fair disclosure: Everybody gets a fair shake in this article, but I've been active in the security industry long enough to accumulate a number of potential conflicts in writing about some of these technologies. Those who want the gory details can see my bio at the end of the story.)

E-Mail Fixes

Without question, two of the most immediate pain points in corporate computing are e-mail-borne viruses and spam. One com-

pany I know recently had multiple computers infected by a virus after a sales manager disabled his antivirus software. He turned off the software because it interfered with another program that the manager needed to run. Next year, rather than leave their security in the hands of end users, more and more companies will institute antivirus scanning in their mail servers, their firewalls and even their routers. In the meantime, companies are looking for technology that automatically installs and updates antivirus software without needing any assistance from the PC user.

As for spam, so long as legislators twiddle their thumbs (and probably even if they stop), the amount of unsolicited e-mail circulating through the Internet will only increase. Already a serious problem for Internet service providers—more than 80 percent of the e-mail received by Hotmail is spam—spam is a growing issue for businesses as well. Companies will increasingly see spam as a security problem and move to widely deploy antispam tools.

The best technologies will combine antispam with antivirus, as Brightmail already does. Until then, spam-only solutions like ChoiceMail, SpamAssassin, Spamnix and SpamSubtract are sure to be quite popular. And while antispam services like SpamCop may remain popular with end users, I believe that businesses will shy away from those services, since they require that each e-mail mes-

mail and your e-mail passwords. What guarantee do you have that these programs are not surreptitiously copying this information and sending it somewhere else? The answer is that there are no guarantees unless the source code of the programs is professionally evaluated—and that is one of the reasons behind the perennial push for evaluated software, the Common Criteria and trustworthy operating systems. Expect to see an increased attention to that kind of formal evaluation applied across many different categories of security tools.

Sleuthware

Forensics is likely to be a huge growth area during the coming year. Today, disk forensic programs are popularly used by law enforcement to discover what was on a suspect's hard drive, as well as by attorneys involved in litigation and discovery to search for documents that the other side might possibly be hiding. I expect that as the understanding of these tools grows, many businesses will use them for investigating the computers of problem employees—both before and after termination.

Today, disk forensic tools are divided into high-end programs like Encase, low-end tools like Norton Utilities and free software like @Stake's Task. What's needed are more midrange tools built around specific problems that people want to solve, rather than specific capabilities that programmers have been able

ees stayed late in the office and spent the night copying files from people's computers to some website in Argentina, would you ever find out? For most businesses, the answer is no. That's because most businesses simply do not monitor what information is passing over their Internet connection. That leads us to the next hot area for 2003: network forensics analysis tools (NFAT). Right now, several such tools exist on the market, including Net-Detector, NetIntercept, NetWitness, NFR, SilentRunner and the open-source program Ethereal. All of these products will capture every packet that moves across your Internet connection and then allow you to reassemble TCP/IP connections so that you can really understand what's going on.

These tools also have their limitations. Unfortunately, with the exception of NetWitness, the current generation is mostly reactive, rather than proactive. Unlike intrusion detection systems, these NFATs don't terminate questionable connections that are in progress. Instead, they simply record everything, under the general assumption that somebody in your organization might want to do something with the data at some later point in time.

The problem here is that you need to know when to go looking for something. For those of us who are naturally nosy, that's no problem. Even so, most organizations will find that having an NFAT creates an ongoing requirement for additional man power—and that translates into an ongoing expense. The next generation of NFATs will need to be better at learning baseline behavior and automatically reporting abnormalities if they are to be broadly adopted.

This push for higher-level functionality and focusing on specific tasks is already appearing in the world of security scanners. A few years ago, I ran Internet Security Systems' Internet Scanner on a small network, and I ended up with a report of more than 100 pages about potential security problems on the network. New tools such as FoundScan will combine problem detection with intelligent prioritization, tracking and remediation reports. In other words, more and more scanners will start checking to see if the problems they detect are actually fixed—and that those problems they detect stay fixed.



Unfortunately, with the exception of NetWitness, the current generation of network forensic tools is mostly reactive, rather than proactive.

sage be sent offsite for antispam processing—a move that potentially threatens business and client confidentiality.

Astute readers are sure to realize that the confidentiality problems inherent in sending e-mail to another company are also present when you use another company's products on your confidential data behind your firewall. Antispam programs that filter your e-mail necessarily have access to your

to develop. We need tools that can run off a bootable CD-ROM so that they can be used without disturbing the host operating system but still have full access to the Internet so that recovered documents can easily be copied to another machine without resorting to sneakernet or CDRs. What's more, these tools need to be usable with little or no training.

Unfortunately, forensic tools also make great tools for burglars. If one of your employ-

New security scanners such as FoundScan will combine problem detection with intelligent prioritization, tracking and remediation reports.

The Kitchen Sink

I expect more and more products to be delivered as “appliances,” rather than as software packages that are loaded onto a Windows or Solaris server. The appliance approach lets a single vendor be responsible for the hardware, the software and the embedded operating system. Appliances also reduce the chances that one program might interfere with another, since the only way that appliances should be communicating with each other (or with the outside world) is through well-established TCP/IP protocols.

The troubling thing about this push to appliances is that most appliances turn out to be rack-mounted PCs running Windows, Linux or FreeBSD. The problem here is that all these operating systems have seen significant security vulnerabilities in the past year and all require constant patching and updating to remain secure. My concern is that many companies selling appliances have failed to devise ways for these systems to be updated in the field; instead, they simply equip the appliance with two Ethernet interfaces and recommend that the management interface be installed behind a firewall. Code Red and Nimda both taught us the fallacy of that approach.

Although biometrics and single sign-on systems are sure to see increased sales in the coming year, I don't expect them to be a potent force for most companies. On the other hand, I expect password synchronization systems to make significant inroads. Those systems ease the pain for workers who need to use multiple computers and yet also need to change their passwords on a regular basis to ensure security. Synchronization is a compromise solution, but it's a solution that seems to work.

Risk Consoles

Just when you thought security software was getting simpler, along comes security risk management, a genre of tools whose purpose is to provide CSOs with a *Star Trek*-like dashboard view of information security vulnerabilities and incidents across the enterprise. The idea is not only to oversee the minutiae but also to manage the enterprise's level of risk in a holistic manner.

Well, that's the goal anyway. Bent under the weight of terms like *vulnerability*, *compliance configuration management* and *security event monitoring*, security risk management is still sorting itself out, says Mike Rasmussen, director of research in information security for Giga Information Group. “If only the vendors would stop misusing the terms *risk*, *vulnerability* and *threat*, it would be much easier to understand,” he says.

In the vulnerability and configuration management space is **Archer Technologies' Security2002**, which collects information on network vulnerabilities, baseline configurations and control standards, and distributes them to system administrators. The nice thing about Security2002 is that it includes a security feed on the latest threats, which negates the need for subscriptions to services like BugTraq.

Going one step further, **Cogentric's Alcon** gives prioritized remediation plans for security incidents. It also gives on-demand views of vulnerability, incident and risk ratings; continuous and prioritized updates of security vulnerabilities and threats; accessibility rights to information by all stakeholders; and historical information on threats, complete with time- and event-based comparisons. So if you have an Oracle system and a new Oracle security threat is found, Alcon will tell you about the threat, compare it to past threats, and indicate how and which systems to protect and whether the threat is a top priority.

Finally, I don't expect much breakthrough progress on the encryption front. With the exception of SSL (secure sockets layer), which is both easy to deploy and absolutely vital for securing e-mail delivery, Web transaction and the like, encryption systems are simply too hard to use. That's sad, because file encryption is one of the few ways to minimize the damage that can be caused by a laptop theft. But experience has shown that people protect themselves only against

Qinetiq Trusted Information Management is another vendor playing in this sandbox (ignore the cute spelling and pronounce it “kinetic”).

Xacta's Web C&A product provides another variation on the theme, helping users make their systems compliant with government and industry security certifications. According to Xacta, Web C&A guides users through a step-by-step process to determine risk posture, and assess system and network configuration compliance with applicable regulations, standards and industry best practices. Those are in accordance with the Department of Defense Information Technology Security Certification and Accreditation and the National Information Assurance Certification and Accreditation processes, and the Director of Central Intelligence Directive, as well as those for the Health Insurance Portability and Accountability Act and the Graham-Leach-Bliley Act (better known as HIPAA and GLB, respectively). Xacta's **Commerce Trust** product assesses systems and keeps administrators up-to-date on vulnerabilities to certification compliance.

Ideally, security risk management tools will do all of the above in one tidy package. Steve Katz says this is exactly the type of product he needed in his former CISO positions at Citigroup and Merrill Lynch; he left the practitioner's chair and put out a shingle at Security Risk Solutions, where he consults to Qinetiq and other players in this developing market.

Right now vendors are offering pieces of the pie, but no one has the entire equation down yet, Rasmussen says. “It all needs to merge and create a single product with every aspect of strong security risk management,” he says. That day is not far off—Rasmussen points out the recent partnership of eSecurity and SecurityFocus as emblematic of the field's ongoing consolidation.

—Simone Kaplan

threats that they think are likely, and most people don't expect that their laptop will ever be stolen or misplaced. ■

Simson Garfinkel is a technology writer based near Boston. **Disclosures:** He has spoken at Brightmail conferences, formerly served on InterMute's advisory board and has a “tiny, tiny” ownership in the SpamSubtract product, is a friend and former business associate of Spamnix developer Barry Jaspán, and cofounded Sandstorm Enterprises and helped develop its NetIntercept NFAT tool.

The Best Defense Is a Firing Offense

What's a CSO to do when his tech expert says No to a request? **By Anonymous**

I'VE LEARNED TWO IMPORTANT RULES since becoming a CSO. One: You can't argue with a technology expert. And two: You've got to argue with a technology expert.

I remembered this particular lesson on a Tuesday. It hadn't even been such a bad Tuesday. That is, until Technology Guy came charging into my office.

"Forget it," he says to me, responding to an e-mail I had just sent him. "No way am I going to do that."

"Why?" I ask blankly.

"Because it doesn't make sense," he says. "It's stupid security. And when it fails, I'll end up taking the blame for it."

"Look, it's not your decision," I remind him, "nor is it mine. Big Boss has asked us to open the port in the firewall to support a new business application. You remember Big Boss," I say to him in my most controlled management voice. "He's the one with the big, cushy chair, approves the budget, signs your paycheck...."

"It's still not happening," he tells me, defiantly. "They're using Report Procedure Calls with that application, which require me to open up not *one* port but 2,000 ports, which makes my firewall worthless."

"Nevertheless....," I struggle to inject my own defiance.

"No way," he interrupts. "Not happening." He leans emphatically across my desk and looks me straight in the eye. "Tell *them* to rewrite their damn application, and tell them to use *real* software for a change." Then he storms out of my office before I can say another word.

Hoo boy. Technology Guy should walk a mile in my wing tips. He doesn't get that this issue is nonnegotiable. The ports need to be opened so that the app can run. Period. Firewall or no, we need to solve the app problem first. And there's no way they are going to recode the application—the company has a lot riding on this. I really need Technology Guy to help me out. But he doesn't seem to get the big picture: The business needs to make money to survive. This app will make money. Ergo, we need this app.

I give Technology Guy time to cool off and then walk down to his office. He's still fuming, however. He says there comes a time when every good technology guy has to put his foot down on bad security. Apparently he has chosen this moment. He calls me a wimp for not standing up to corporate. "Nothing personal," he says.

He thinks I should explain to Big Boss that we are all going to die because of security stupidity. I make one last attempt to explain, but he refuses to discuss it any longer. Technically speaking, of course, he's right. But Big Boss doesn't want to hear about security problems—they only cost him time and money.

A conversation with the programming team doesn't help matters either. I explain to them about opening the 2,000 ports and why that might be a problem. Don't they care about my problems with security?

"Not so much," Project Boy tells me. "You should have said something much earlier in the process."

"Really? When?" I wonder to myself. "You've been working on this project for a year. I never heard anything about it until two weeks ago. Where was the security review of the project?" I ask impatiently.

"We didn't do one," he retorts, knowing I'm trapped by



a technicality: "This isn't a security product, so no security review. You were supposed to be kept in the loop by Big Boss. Didn't he tell you about it?" He smiles again. It's obvious that I hadn't heard a word from Big Boss. "Guess you need to take this up with him then," says Project Boy. "But if you don't get those ports open, we'll both end up

in his office. And my project has more priority," he says. And he's right.

Nothing like being the meat in a crap sandwich. So it's back down to talk to Technology Guy.

"Is there *any* solution we could use that will solve the problem of the RPCs through the firewall?" I ask politely.

"Absolutely not," he says. "They'll just have to recode the app. It's the only solution."

Secretly, I find it hard to believe. But I persevere. "I'm sure someone has solved this," I say, not knowing anything for sure at this point.

"Nope," he says. "And I'm an expert when it comes to this sort of thing."

Technology Guy may be an expert, but I'm a manager. Not every CSO may be up to snuff when it comes to technology, but we know other managers and their own technical people. And it's a good way to check out the truth from time to time.

So I call my friend, Manager Maven, at a company across town and explain the situation. He says they had the same problem, but one of his guys came up with a firewall that could deal with RPC calls. Seems that applications using RPCs have to negotiate whichever of the 2,000 ports they're going to use on Port 135, and then they use the negotiated port. RPC firewalls that understand how RPCs work shut down all ports except for the ones where the apps have negotiated a common port between the two. That way, there are no open ports without an actual app attached to them. The other ports aren't available to scanners or hackers that come calling.

I also call Vendor Professional. He has a product available for servers, so we could use the existing firewall and park that software on the host server without disturbing the firewall we have in use. Pretty slick. All we need to do is open the 2,000 ports and then fix them to the IP address for the RPC box, which would not allow the ports to be used with any other server. Problem solved.

Vendor Professional agrees to come by for a demo. Everyone—Big Boss, Technology Guy, Project Boy—are gathered in the conference room. Vendor Professional shows us how his RPC-savvy firewall product would work and offers to install it right away.

Predictably, Technology Guy asks a lot of tech questions, but Vendor Professional is prepared and answers them all. Also predictably, Technology Guy leaves the conference room in a huff. Oh well.

Vendor Professional installs the product on the server and, sure enough, it protects the

to give me the password to the firewall. I may not be an expert, but I know how to open a damn firewall.

"Can't," he tells me. "Technology Guy changed the password on the firewall and won't give it to me, so I can't make the changes you want. He said we have to put our foot

Technology Guy has chosen this moment to put his foot down on bad security and calls me a wimp for not standing up to corporate. "Nothing personal," he says.

server properly, it deals with RPC strangeness, and it works with the existing firewall. Nice job, says Big Boss. Let's make this happen. Happy to do so, I think to myself.

Except for one thing: I need to get Technology Guy to open up the ports on the connection point firewall to talk to the Internet. When I appear in his doorway, he looks up smugly and says, "Told you it wouldn't work."

"Wrong," I say, even more smugly. "It's up and working, and everyone is happy but you. So you need to open up the 2,000 ports and Port 135 and set them to go to the server's IP address only." Smugness aside, I think I should be commended for my good mood given all the grief I had put up with from Technology Guy about the subject.

And that's when it happens. A dark cloud appears over Vesuvius, and...it...blows. "People who don't know anything about security should not be messing in security stuff," Technology Guy rants. I know he means me, even though I am not completely without a clue when it comes to security technology. "This has completely violated corporate policy," he says. "No one understands the dangers this will unleash." It was almost tragic.

Still, he sticks to his guns and refuses to open the ports in the firewall. I ask him politely—one more time—and still he refuses. As a manager, I know that, in a deadlocked situation, a leader has to make a decision. Yes or no. A nondecision *becomes* a decision, and the factors will spin off in an uncontrollable way. In this case, I decide *yes*, we will make the changes and *no*, I don't need Technology Guy to do it. I track down his backup and ask him

down on bad security practices."

That so, huh? I call the firewall vendor and ask how to get the password out of the firewall if the security manager won't give it up. It won't be easy, they tell me, but it can be done. I have them back up and look over everything to make sure there are no back doors or other issues. "Nope, none," they confirm, and even offer that the firewall looks as if it has been meticulously maintained.

When Technology Guy comes back from lunch, he loses it again. "I told you we could not make those changes," he shouts.

"I know," I say quietly. It's amazing how easy it is to keep your cool when you're in control. "You already said that. You also said there was no solution to the RPC problem. You said the solution wouldn't work, and it did. Then you refused to help out with alternative solutions. Why?" I ask.

"Someone has to put their foot down and keep the company from killing itself," he says. "You're not the only one who can backdoor a firewall. So if you changed the password on the firewall, I'll just change it back."

And that's when I remember the third important rule. When dealing with difficult, uncompromising, domineering, pig-headed people, sometimes you just gotta do what you gotta do.

"If that's the way you feel about it, I am truly sorry," I tell Technology Guy. "You're fired." Nothing personal. ■

This column is written anonymously by a real CSO at a major corporation. To send feedback, e-mail us at csoundercover@cxo.com.

Sales and Services

CSO Sales Offices

President Walter Manninen • 508 935-4101
Group Publisher
Gary J. Beach • 508 935-4202
Publisher Bob Bragdon • 508 935-4443
Executive VP Sales/Custom Publishing
Ellen Romanow • 508 935-4796

East Coast

Senior VP Sales/East
Michael J. Masters • 973 244-4040
Eastern Regional Sales Manager
Paul Reiss • 508 935-4163
Senior Regional Manager
Kathy Powers • 973 244-4041
Regional Sales Manager
Ellie Schwab • 973 244-4042
Account Executives
Joan Bonadeo • 973 244-4043
Gale Tedeschi • 973 244-4031
Advertising Sales Associates
Rhonda Goodman • 973 244-4033
Sharon Patrick • 973 244-4044

New England

Senior Regional Manager/Advertising Sales
Len Ganz • 508 935-4039
Account Executive Kim Forrest •
508 935-4068
Senior Advertising Sales Associate
Dawn Cora • 508 935-4092,
Fax 508 879-6063

Mid-Atlantic

Senior Regional Manager/Advertising Sales
Louise Cupelli • 215 627-8114
Account Executive
Maureen Welsh • 215 627-8114
Advertising Sales Associate
Meredith Hagan • 215 627-8114

Midwest

Regional Director
Robert E. Sawdon • 512 306-9801
Regional Sales Manager
Christopher Nolan • 847 441-5005
District Sales Manager
Beth Carlson • 847 441-3140
Senior Advertising Sales Associate
Brenda Garza • 512 306-9801,
Fax 512 306-9805
Advertising Sales Associate
Kim Giovanni • 847 441-5005

West Coast

VP Sales/West
Cheri McKeithan • 415 975-2685
Senior Regional Manager/Advertising Sales
Jane Evans • 415 975-2680
Regional Manager/Advertising Sales
Ai Collins • 415 975-2686
Account Executives
Derek Jung • 415 975-2683
Tom Ocampo • 415 975-2693

Southern California

Regional Sales Manager Chris Bramel •
949 475-5579
Account Executive Isaac Ugay •
949 475-5579, Fax 949 475-5583

List Services

List Services Director
Kathryn A.W. Marston • 508 935-4072
List Services Account Executive
Stephanie Roy • 508 935-4151
List Services Coordinator
Kim Cormican • 508 935-4152

Online Services

VP/Online Sales
Lisa Brown • 508 935-4470
Online Sales Mgr.
Michael McPhee • 508 935-4611



THE RESOURCE FOR SECURITY EXECUTIVES

Custom Publishing

Group Director Michael Siggins
Director Mary Gregory
Director of Content Development Tom Field
Project Manager Amy Greenleaf
Graphic Designer Chris Brown

Production

VP/Manufacturing Chris Cuoco
Production Manager Lee Tuttle
Ad Production Coordinator Lisa Stevenson

Executive Programs

Senior Vice President Ronald L. Milton
VP, Conference Management Cynthia Mollus
Director, Marketing Services
Shellie Rapson James
Director of Sales John Amato
Manager, Program Operations Brian Fuce
Manager, Procurement/Tech. Planning
Cynthia Laird
Event Development Specialist
Sandra J. Hughey
Program Applications Specialist
Heather Beauton (Senior)
Operations Coordinator Michael Barbato
Fulfillment Services Coordinator
Andrea Slobogan
Manager, Event Planning Amy Turell

Marketing

Executive VP/Marketing
Cathy O'Leary Hayes
VP/News and Information Susan Watson
Media Relations Manager Karen Fogerty
News and Information Assistant
Lori Piscatelli
Marketing Research Director
Bridget Cammarata
Marketing Research Manager
Carolyn Johnson
Sr. Marketing Research Analyst
Dylan DiGregorio
Marketing Comm. Director Sue Yanovitch
Sr. MarCom Development Specialist
Kari Curto
Marketing Comm. Coordinator
Sarah Crowley

Circulation

Senior VP/Circulation Carol A. Spach
Circulation Promotion Manager
Faith Marcello
Circulation Fulfillment Manager
Valerie Szymanski
Subscription Svcs. Supervisor Tina Pescaro
Circulation Fulfillment Assistant
Diana Turco

Reprint Services

For article reprints, please contact Reprint
Services at 651 582-3800 or e-mail
csoreprints@reprintservices.com.
For further sales information, visit
www.csoonline.com/marketing/sales.html.

CSO Contact Information

Editorial, Advertising and Business Offices

492 Old Connecticut Path, P.O. Box 9208,
Framingham, MA 01701-9208, 508 872-0080.

Postal Information

CSO (ISSN 1540-904x) is published
monthly by CXO Media Inc., 492 Old Con-
necticut Path, P.O. Box 9208, Framingham,
MA 01701-9208. Application to mail at Peri-
odicals postage rate is pending at Framing-
ham, MA 01701, and at additional mailing
offices. Canadian Publications Mail agree-
ment number 1902075. CANADIAN POST-
MASTER: Please return undeliverable copy
to P.O. Box 1632, Windsor, ON N9A7C9.

Permissions

Copyright 2002 by CXO Media Inc. All rights
reserved. Reproduction of material appear-
ing in CSO is forbidden without written per-
mission. Send all requests to Permissions
Department, CSO, 492 Old Connecticut
Path, P.O. Box 9208, Framingham, MA
01701-9208.

Photocopy Rights

Permission to photocopy for internal or per-
sonal use or the internal or personal use of
specific clients is granted by CSO for users
through the Copyright Clearance Center,
provided that the base fee of \$3 per copy of
the article, plus \$.50 per page is paid
directly to Copyright Clearance Center, 27
Congress Street, Salem, MA 01970. Please
specify: ISSN 1540-904x. Permission to
photocopy does not extend to contributed
articles followed by this symbol: ‡.

Subscriptions

Address inquiries to CSO, P.O. Box 3482,
Northbrook, IL 60065; 866 354-1125. CSO is
free to qualified information executives. To
all others the one-year basic rate is \$90 for
the United States and Canada, \$115 to for-
eign countries (payable in U.S. funds only).
The single copy price is \$9. Please allow
four to six weeks for new subscriptions to
begin.

Change of Address

Please go to www.omed.com/custsrv/cso
and follow the online instructions.

Postmaster

Send change of address to CSO, P.O. Box
3482, Northbrook, IL 60065. Printed in the
USA.

Index of Companies and Advertisers

Page numbers refer to the first page of
the article(s) in which the company is
mentioned. This index is provided as a
service to readers. The publisher does not
assume any liability for errors or omissions.

Company Index

@Stake Inc.	30
American International Group Inc.	50
Aon Corp.	30, 40
Archer Technologies LLC	57
Banc One Investment Management Group	15
Booz, Allen & Hamilton	38
Central DuPage Health	38
Chubb Group of Insurance Companies, The	50
Cogentrix	57
Computer Economics Inc.	40, 50
Computer Security Institute	40
Counterpane Internet Security Inc.	15
Defcom Information Security Ltd.	15
Defensive Thinking Inc.	15
Delphi Group	28, 30
Exostar LLC.	30
Gartner	30, 40
Giga Information Group Inc.	57
Guy Carpenter & Co. Inc.	50
Hydro One Networks Inc.	15
International Security Technology Inc.	30
Internet Trading Technologies Inc.	40
KeyCorp	15
Lloyd's of London	50
Marsh & McLennan Companies Inc.	50
MassMutual Financial Group	15
Nasdaq Stock Market Inc., The	24
Northrop Grumman Information Technology	15
Ohio Savings Bank	15
Omni Consulting Group	44
Pacific Life Insurance	15
QinetiQ PLC	57
Riptech Inc.	30
Security Risk Solutions LLC	57
St. Paul Companies Inc., The	50
Texas Instruments Inc.	15
Trigger Street Productions Inc.	15
TruSecure Corp.	50
Xacta Corp.	57
Ziff Davis Media Inc.	40
Zurich North America	50, 64

Advertiser Index

ADT	25
Avaya	23
BearingPoint Inc.	7
Check Point Software	32
Computer Associates Intl. Inc.	5
CXO Media Inc.	49, 56
CyberGuard Corp.	17
GROUP	53, 55
IBM Corp.	27
Information Security Executive Awards	63
Lancope Inc.	C3
Netscreen Technologies Inc.	11
Nokia	12
OKENA	37
PentaSafe	C4
PricewaterhouseCoopers	9
SAVVIS	14
Symantec Corp.	2
TippingPoint Technologies Inc.	C2
Unisys Corp.	19
VeriSign Inc.	21



invites you to

Celebrate Georgia's Information Security Pioneers

Information Security Executive of the Year in Georgia™ Award honors the achievements of today's information security pioneers and recognizes excellence in managing enterprise-wide network and Internet security systems. Join us at Atlanta's historic Fox Theatre on March 19, 2003, when we celebrate these forward-thinking individuals.

Call for Nominations

Nominate your Chief Security Officer, or executive in an equivalent position, for the Information Security Executive of the Year in Georgia for 2003. Nomination forms are currently available online at www.infosecaward.com.

Call for Sponsors

Only a few sponsorship packages remain! Take this opportunity to participate in this premier event for Georgia's most innovative information security professionals. Visit www.infosecaward.com for updated sponsorship package information.



Keynote Speaker :



Richard Marshall
*Principal Deputy Director,
Critical Infrastructure
Assurance Office (CIAO)*

gigabyte sponsors

STONESOFT



INTERNET
SECURITY
SYSTEMS™

megabyte sponsors

Lancope



PEOPLE
NETWORK INC

media sponsors

CSO
THE RESOURCE FOR SECURITY EXECUTIVES
CSOonline.com

TechLINKS
THE GUIDE TO TECHNOLOGY IN GEORGIA

www.infosecaward.com

info@infosecaward.com

404.982.8562

debriefing

Pop Quiz



Chances Are...

1. What is the estimated cost to insurance companies resulting from 9/11?

- a. \$5.5 billion b. \$19.6 billion
- c. \$40.2 billion d. \$80.3 billion

2. What was the cost of the next biggest insurance event ever, Hurricane Andrew?

- a. \$5.5 billion b. \$19.6 billion
- c. \$40.2 billion d. \$80.3 billion

Of the 20 most expensive insurance events of 2000:

- 3. How many were computer related?**
- 4. How many were weather related?**

5. What premium does Zurich North America estimate a bank with \$5 billion in assets will pay for cybersecurity insurance?

- a. \$100 million b. \$10 million
- c. \$1 million d. \$275,000

6. If all Fortune 1000 companies in America bought that level of coverage, they would pay a combined premium of \$275 million,

an amount of money equal to what?

- a. The amount needed to certify about 611,000 CISSPs
- b. The daily losses to airlines following 9/11
- c. Roughly one-tenth the estimated losses from the Nimda virus
- d. All of the above

7. About how many lines of code are required to eliminate the occurrence of a buffer overflow in software?

- a. 1 b. 135 c. 1,100 d. 6,000

8. According to experts, what percentage of computer attacks would that eliminate?

- a. 5 b. 10 c. 15 d. 60

9. What is the significance of "B<PL"?

- a. It's the pseudonym of the hacker who defaced the Girl Scout's website

- b. It's a rule for creating elliptic curve encryption where B is binary code that must equal less than the product of P packets and L loose strings
- c. It's the classic formula for determining negligence where B is cost of prevention, P is probability of a bad event and L is the amount of loss from the event
- d. It's the one line of code required to eliminate a buffer overflow

10. True or False: A major corporation has been found guilty of negligence due to information security shortcomings.

11. According to the Center for National Software Studies, the odds a company will admit to being hacked are about the same as what?

- a. The odds of arriving at a traffic light when it's green, 1 in 3
- b. The odds of being hurt in a car accident, 1 in 75
- c. The odds a golfer will sink a hole in one, 1 in 10,700
- d. The odds of being struck by lightning, 1 in 600,000

12. The odds of a company being attacked by hackers are about the same as what?

- a. The odds of starring in a movie, 1 in 385,000
- b. The odds of a pregnant woman having twins, 1 in 50
- c. The odds you'll wear glasses in your lifetime, 1 in 2
- d. The odds you'll die, 1 in 1

13. Complete the following quote [by Andrew Lang]: "An unsophisticated forecaster uses statistics as..."

- a. a way to fudge forecasts."
- b. an excuse for research and an explanation for failure."
- c. a drunken man uses lampposts—for support rather than for illumination."
- d. the basis for inflated insurance rates."

ANSWERS: 1. C 2. B 3. D 4. 15 5. D 6. D 7. A 8. D 9. C 10. FALSE 11. A 12. D 13. C

How'd You Do?

0-5 correct: You should take Actuarial Science 101

6-12 correct: You should teach Actuarial Science 101

13 correct: Chances are, you cheated



Lancope

I'VE BEEN
HIRED TO
STEAL YOUR
DATA.

TRY TO
STOP ME.



Advanced Threat Management

StealthWatch™ by Lancope does more than use signatures to detect network attacks.

As the most versatile IDS available, StealthWatch is a behavior-based Intrusion Detection System that prevents internal misuse on your network and provides bi-directional protection against known, unknown, mutated, encrypted and DoS attacks. More than an IDS, StealthWatch gives an unparalleled view of network activity for optimal bandwidth and policy management.

Request your free White Paper ***Security Benefits of Behavior-Based IDS*** at <http://www.lancope.com>.

StealthWatch and Lancope are Registered Trademarks of Lancope, Inc.



"V" is for VigilEnt Integrated Security Management Solutions from PentaSafe.

**TERRY MCMULLEN, General Manager,
Jack Henry & Associates,
PentaSafe customer**

Jack Henry & Associates is VigilEnt with PentaSafe.



PENTASAFE SOLUTIONS

As General Manager of Electronic Services at Jack Henry & Associates, I'm responsible for the data processing of hundreds of banks and financial institutions-nationwide. Our business and our clients demand the highest security standards. Since 1999, we've relied on PentaSafe's VigilEnt software to help us secure millions of transactions everyday.

See for yourself how PentaSafe security solutions can help you become more vigilant in managing security across your enterprise.

Want to find out more about PentaSafe's VigilEnt Integrated Security Management Solutions?

Go to www.pentasafer.com to:

- Register for an Executive Security Briefing, featuring Gartner Group's John Pescatore.
- Download our free "Integrated Security Management" whitepaper



PentaSafe

The safest way to grow your business.